2006-12

Simulation and performance analysis of routing in SONET/SDH Data Communications Network (DCN)

Loh, Kuan Chou.

Monterey California. Naval Postgraduate School

http://hdl.handle.net/10945/2482

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SIMULATION AND PERFORMANCE ANALYSIS OF ROUTING IN SONET/SDH DATA COMMUNICATIONS NETWORK (DCN)

by

Kuan Chou Loh

December 2006

Thesis Advisor: John C. McEachen
Second Reader: Randy L. Borchardt

Approved for public release, distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Simulation and Performance Analysis of Routing in SONET/SDH Data Communications Network (DCN)			**5. FUNDING NUMBERS**
6. AUTHOR(S) Kuan Chou Loh			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT *(maximum 200 words)*

This thesis analyzes the ITU-T G.7712 standard to evaluate the main features and specifications that are defined in the 11/2001 edition. The latest 03/2003 revision was also reviewed to determine what are the changes and latest update presented in that paper. In order to find out the compliance among telecommunication industry vendors, surveys were also conducted to determine which is the most widely supported standard. Finally, simulations were run using Opnet IT Guru software for the two routing protocols defined in the standard, IS-IS and OSPF, to examine their characteristics and determine their usefulness. It was observed that OSPF achieves better performance and is the least obtrusive on network operations.

14. SUBJECT TERMS Network Management Protocols, SNMP, CMIP, SONET, Optical Networks, Data Communication Channels, Scalability Issues, Traffic Analysis and OPNET Simulation.			**15. NUMBER OF PAGES** 91
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

SIMULATION AND PERFORMANCE ANALYSIS OF ROUTING IN SONET/SDH DATA COMMUNICATIONS NETWORK (DCN)

Kuan Chou Loh
Civilian, Ministry of Defense, Singapore
Bachelor of Engineering (Hons), Nanyang Technological University, Singapore, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 2006

Author: Kuan Chou Loh

Approved by: John C. McEachen
Thesis Advisor

Randy L. Borchardt
Second Reader

Jeffrey B. Knorr
Chairman, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis analyzes the ITU-T G.7712 standard to evaluate the main features and specifications that are defined in the 11/2001 edition. The latest 03/2003 revision was also reviewed to determine what are the changes and latest update presented in that paper. In order to find out the compliance among telecommunication industry vendors, surveys were also conducted to determine which is the most widely supported standard. Finally, simulations were run using Opnet IT Guru software for the two routing protocols defined in the standard, IS-IS and OSPF to examine of their characteristics and determine their usefulness. It was observed that OSPF achieves better performance and is the least obtrusive on network operations.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would first like to thank my wife Jerin for all of her support during the past one and one-half years. Without her help and understanding regarding my time spent at preparing the thesis, this would have been a much more difficult task. I would like to express my most sincere gratitude to Prof. John McEachen for his guidance and providing me with the resources necessary to conduct this study as effectively as possible. He has never failed to response to my questions and I really appreciate it.

I would also like to thank Prof. Randy Borchardt for agreeing to be my second reader to this thesis and also providing support and guidance.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) standard has evolved from a relatively unknown technology in the 1980s to become widely deployed throughout the telecommunications industry. Several ITU-T standards have been published to ensure standard protocols and recommendations are followed by all equipment vendors on how the network should perform.

ITU-T G.7712 is the standard for Architecture and Specification of the Data Communications Network (DCN). It is used for network management, signaling and routing traffic in SONET/SDH, Optical Transport Network (OTN) and Dense Wavelength Division Multiplexing (DWDM) networks.

G.7712 is important for the telecommunication industry since it enables intelligent optical networks with combined IP-managed and OSI-managed equipment. It is also crucial for vendors of network edge devices as it allows for easy transport of network management traffic to these devices via the core optical switches without the need to create expensive and complicated overlay networks.

The first part of this thesis research is to look into the ITU-T G.7712 standard to find out what are the main features and specifications that were defined in the 11/2001 edition. The latest 03/2003 revision was also reviewed to determine what changes and updates were presented in that paper.

A survey was done to determine the support of the ITU-T G.7712 standard by some of the major SONET/SDH vendors in the telecommunications industry. Five vendors were selected and the results will show the support level of these vendors.

The second part of this thesis research is to model and simulate the DCN using OPNET IT Guru software for the two routing protocols defined in the standard, IS-IS and OSPF.

OPNET IT Guru is a modeling and simulation tool that provides an environment for analysis of communication networks. However, it does not have a SONET Data Communications Channel (DCC) model in its standard model library. Thus a SONET DCC network model was created to facilitate our simulation of IS-IS and OSPF routing protocols as defined in the G.7712 standard.

Three different scenarios were created using this OPNET model to simulate the packet flow within the SONET DCC network and to understand the differences and characteristics of the two routing protocols. The objective of each experiment scenario was to evaluate the performance using parameters like Ethernet delay, server performance, link throughput and link utilization.

The overall results demonstrated that OSPF is the protocol most suited for the DCC network based on its performance. It also supports the decision of G.7712 in specifying the use of an IP protocol architecture for the DCC network.

I. INTRODUCTION

A. BACKGROUND

Before the birth of Synchronous Optical Network (SONET) / Synchronous Digital Hierarchy (SDH), the transmission system widely deployed in the telecommunications industry was known as the Plesiochronous Digital Hierarchy (PDH) [1]. Plesiochronous means the timing of signals across the network is almost but not precise, and there is not a centralized timing source since each node has its own clock.

As more and more channels were multiplexed together into higher layers of the PDH hierarchy, each frame need to be completely demultiplexed in order to select an individual channel as the timing across all the nodes was not totally the same. Another problem occurred where different networks with relatively wide differences in timing met, such as between Europe and the U.S.

The SONET standard was designed in the mid 1980's to alleviate these problems [1]. It is more widely used in North America. The International Telecommunications Union later generalized SONET into the SDH in order to accommodate the PDH rates in use outside North America, mainly deployed in Europe and Asia-Pacific Countries.

SONET/SDH standardized the line rates, coding schemes, bit-rate hierarchies, and operations and maintenance functionality. SONET/SDH also defined the types of Network Elements (NEs) required, network architectures that vendors could implement, and the functionality that each node must perform.

A typical SONET/SDH network utilizes the Section Data Communications Channels (DCC). Briefly, one or more Operations Systems (OSs) manages the SONET/SDH NEs and the connectivity between them is achieved through a Data Communications Network (DCN).

Open System Interface (OSI) was selected as the standard for SONET Section DCC because OSI protocols were accepted as the basis for the larger set of Telecommunications Management Network (TMN) standards.

Compared to OSI, the Simple Network Management Protocol (SNMP) layers are much simpler. In SNMP, the network management applications consist of vendor-specific modules such as fault management, log control, security and audit trails and they map the SNMP management traffic instead of OSI headers into the DCC fields or the payload areas for onward transmission to the management process.

Because of the simplicity and similarity of the SNMP network management process, service providers have begun to request that SONET/SDH products support an IP protocol stack on their OS/NE interface (Ethernet), since many service providers did not want to implement an OSI-based DCN or deploy mediation devices.

G.7712 is the standard for Architecture and Specification of the Data Communications network (DCN) [2]. G.7712 is important for the telecommunication industry since it enables intelligent optical networks with combined IP-managed and OSI-managed equipment. It is also crucial for vendors of network edge devices as it allows for easy transport of network management traffic to these devices via the core optical switches without the need to create expensive and complicated overlay networks.

B. OBJECTIVES

There are 2 main objectives of this thesis. The first one involved study into the main features and new updates available in the ITU-T G.7712 standard and a survey was done to determine the support level by some of the major SONET/SDH vendors in the telecommunications industry. The push for an eventual IP DCN for managing the SONET network is obvious as shown by the positive support from the telecommunications industry.

As such, it is necessary to evaluate the routing protocols in the DCN to facilitate moving towards an IP DCN and this formed the second objective of this thesis. By modeling and simulating the two routing protocols in the DCN using OPNET IT Guru, the overall results demonstrated that OSPF is the protocol most

suited for the DCC network based on its performance. It also supports the decision of G.7712 in specifying the use of an IP protocol architecture for the DCC network.

C. RELATED WORK

So far, no one has done any related research of this nature based on an in-depth literature survey. Further, a search via the internet cannot find any similar studies. By doing this study, we can determine whether this standard is widely adopted by the telecommunications industry and, if so, it will help in defining the protocols when designing a DCN to manage the SONET/SDH network.

D. THESIS ORGANISATION

This chapter provides a brief background of SONET/SDH and the objective of this thesis. The following paragraphs explained how the various chapters of this thesis report are being organised.

Chapters II and III provide some background knowledge for understanding the Synchronous Optical Network (SONET) / Synchronous Digital Hierarchy (SDH) technologies. Chapters IV and V examine the protocols used by the SONET/SDH network management and analyze the ITU-T G.7712 standard to find out its main tenets, which is the main objective of this thesis research. Chapter VI concludes the thesis.

In Chapter II, a brief history on how SONET/SDH has evolved from a relatively unknown technology to become widely deployed in the telecommunications industry is presented. This is followed by some of the advantages and usefulness of SONET/SDH. The chapter ends with the main differences between SONET and SDH.

The basic configuration and terminology associated with the equipment of a simple SONET network are explained in Chapter III. The SONET architecture, multiplexing hierarchy, its frame structure, functions of the overhead bytes, and

how are they are being used in the SONET built-in standards for Operations, Administration, Maintenance and Provisioning (OAM&P) are also presented in this chapter.

Chapter IV focused on the main objective of this thesis research. Definitions and usage of Data Communications Channel (DCC) and Data Communications Network (DCN) are explained. The two main protocols used by the network management of SONET/SDH, Open System Interface (OSI) and Simple Network Management Protocol (SNMP) using Internet Protocol (IP) are also explored, followed by a comparison between the two of them and why there is a push for IP over the DCC. The chapter concludes with the study into the main features and new updates available in both the 11/2001 and 03/2003 edition of the ITU-T G.7712 standard.

The outcome of the surveys to determine the compliance among telecommunication industry vendors are presented in Chapter V. Finally, an Opnet model was created to study the two different routing protocols, IS-IS and OSPF defined in the G.7712 standard.

Chapter VI concludes the thesis report with outcome of the research and what future research areas can be further explored.

II. BACKGROUND

A. CHAPTER OVERVIEW

In this chapter, we will look at the evolution of Synchronous Optical Network (SONET) / Synchronous Digital Hierarchy (SDH) from a relatively unknown technology to become widely deployed in the telecommunications industries. We will then list out some of the advantages and usefulness of SONET/SDH. The main differences between SONET and SDH will also be presented.

B. SONET/SDH EVOLUTION

In the early 1980s, a revolution in telecommunications networks was ignited by the use of a relatively unassuming technology, fiber-optic cable. Since then, the consequential increase in network quality and tremendous cost savings have led to many advances in technologies required for optical networks. Many of these benefits have yet to be realized. The digital communications network has evolved through three fundamental stages: asynchronous, synchronous, and optical.

1. Asynchronous

Traditional digital telecommunications services such as T1/DS1s were designed to aggregate analog telephone lines for more efficient transport between central offices. Twenty four digitized voice lines (DS0s) were carried over a DS1 using time-division multiplexing (TDM).

To review, in a TDM architecture, multiple channels (24 for DS0) share the circuit basically in rotation, with each DS0 having its own assigned time slot to use or not as the case may be [1]. As each channel is always found in the same place no address is needed to demultiplex that channel at the destination. Twenty-eight (28) DS1s are TDM aggregated into a DS3 in the same manner.

The older DS1/DS3 system is known as the Plesiochronous Digital Hierarchy (PDH), as the timing of signals across the network is plesiochronous,

which means almost but not precisely. Data communications networks such as Ethernet are asynchronous, as there is not a centralized timing source and each node has its own clock.

As more and more channels are multiplexed together into higher layers of the PDH hierarchy, a number of problems arise. Since the timing on various DS1s going into a DS3 may differ slightly, bit-stuffing is required to align all within the DS3 frame. Once this is done, the individual DS1s are no longer visible unless the DS3 is completely demultiplexed. In order to select an individual channel, the whole DS3 frame must be torn down to extract out the DS1 and then subsequently rebuilt back into the DS3. The equipment required to do this is expensive. Another problem arises with interoperability of different networks with relatively wide differences in timing, such as those in Europe and the U.S.. Expensive equipment that also adds latency is required for the interface.

2. Synchronous

To alleviate these problems, the Synchronous Optical Network (SONET) standard was designed in the mid 1980’s [1]. It is more widely used in North America. The International Telecommunications Union later generalized SONET into the Synchronous Digital Hierarchy (SDH) in order to accommodate the PDH rates in use outside North America, mainly deployed in Europe and Asia-Pacific Countries.

SONET/SDH standardized line rates, coding schemes, bit-rate hierarchies, and operations and maintenance functionality. SONET/SDH also defined the types of network elements required, network architectures that vendors could implement, and the functionality that each node must perform. Network providers could now use different vendor's optical equipment with the confidence of at least basic interoperability.

3. Optical

The one aspect of SONET/SDH that has allowed it to survive during a time of tremendous changes in network capacity needs is its scalability. Based on its open-ended growth plan for higher bit rates, theoretically no upper limit exists for SONET/SDH bit rates (The current maximum bit rate deployed is

40 Gbps). However, as higher bit rates are used, physical limitations in the laser sources and optical fiber begin to make the practice of endlessly increasing the bit rate on each signal an impractical solution. Additionally, connection to the networks through access rings has also had increased requirements. Customers are demanding more services and options and are carrying more and different types of data traffic. To provide full end-to-end connectivity, a new paradigm was needed to meet all the high-capacity and varied needs. Optical networks provide such bandwidth and flexibility to enable end-to-end wavelength services.

Optical networks began with wavelength division multiplexing (WDM) [1], which arose to provide additional capacity on existing fibers. Like SONET/SDH, defined network elements and architectures provide the basis of the optical network. However, unlike SONET/SDH, rather than using a defined bit-rate and frame structure as its basic building block, the optical network will be based on wavelengths. The components of the optical network will be defined according to how the wavelengths are transmitted, groomed, or implemented in the network. Viewing the network from a layered approach, the optical network requires the addition of an optical layer. To help define network functionality, networks are divided into several different physical or virtual layers. The first layer, the services layer, is where the services such as data traffic enter the telecommunications network. The next layer, SONET/SDH, provides restoration, performance monitoring, and provisioning that is transparent to the first layer.

Emerging with the optical network is a third layer, the optical layer. Standards are being developed and essentially can provide the same functionality as the SONET/SDH layer, while operating entirely in the optical domain. The optical network also has the additional requirement of carrying varied types of high bit-rate non-SONET/SDH optical signals that bypass the SONET/SDH layer altogether. Just as the SONET/SDH layer is transparent to the services layer, the optical layer will ideally be transparent to the SONET/SDH layer, providing restoration, performance monitoring, and provisioning of individual wavelengths instead of electrical SONET/SDH signals.

C. ADVANTAGES OF SONET/SDH

There are a number of advantages of deploying a SONET/SDH network, for both the customers and service providers. Each of the key benefits is briefly explain below:

1. Multipoint Configuration

SONET/SDH is frequently deployed in multipoint configurations. This means several sources of SONET/SDH traffic can be combined and distributed without terminating the digital stream to recover and process the constituent signals. This process is also known as “grooming”. Grooming can concentrate traffic and service more customers with fewer links than without grooming. SONET/SDH grooming requires less equipment, thus reducing the need for linking multiplexers, digital cross-connect and the need for cabling between equipment terminations and patch panels. In simple terms, it also means saving space and money.

2. Enhanced Operations, Administration, Maintenance and Provisioning (OAM&P)

SONET/SDH enhances the OAM&P capabilities and integrates them into all SONET/SDH network elements, mostly through the inclusion of dedicated overhead bytes reserved for the purpose. The OAM&P procedures are an integral part of the SONET/SDH standard with more bandwidth allocated for them and thus the information available is more sophisticated. This substantial amount of information available allows for quicker troubleshooting and detection of failures before the network degrades to unacceptable levels. It also allows for remote provisioning and configuring of SONET/SDH network elements, and thus can be centrally maintained without disturbing the link and services to the users and indeed reduces the travel expenses for maintenance personnel.

3. New Service Offerings

The huge amount of bandwidth available in SONET/SDH can support new services that were not possible previously. Video applications, 100 Mbps LAN interconnections, color faxing, and other bandwidth-hungry applications are now easily supported in an affordable and reliable mean.

4. Optical Interface

Optical interconnect, also known as “mid-span meet” is made possible with multi-vendor compatibility since the SONET/SDH standards are well defined for fiber-to-fiber interfaces at the physical (photonic) layer. These low level aspects define the optical line rate, wavelength, power levels, pulse shapes, and coding for bits on the fiber links. They allow the customer to use a direct SONET/SDH interface, possibly a different vendor equipment to connect to its service provider.

5. Protection Rings

The ability of SONET/SDH to be deployed in a ring architecture is perhaps the most distinctive feature of SONET/SDH network. It enables the SONET/SDH network to configure various types of protection mechanisms: Unidirectional Line-Switched Rings (ULSR), Unidirectional Line-Switched Rings (ULSR), Two-Fiber Bidirectional Line-Switched Rings (2F-BLSR) and Four-Fiber Bidirectional Line-Switched Rings (4F-BLSR) based on a given requirement. No matter which mechanism the SONET/SDH network employs, the main objective is to allow the automatic protection switching to kick in when a failure is detected and restore the services to the customers without any noticeable interruption to the traffic.

D. DIFFERENCES BETWEEN SONET AND SDH

There are basically only two major differences between SONET and SDH [3], the first one is the naming convention/hierarchical structure for the transmission rates and the second being the framing used for the overhead bytes.

1. Naming Convention

Table 1 shows the difference transmission rates between SONET and SDH.

Common SONET/SDH Rates			
Speed	SONET (US)	SDH (Europe)	OCx (ATM)
51.84 Mbps	STS-1	STM-0	OC-1

155.52 Mbps	STS-3	STM-1	OC-3
622.08 Mbps	STS-12	STM-4	OC-12
2488.32 Mbps	STS-48	STM-16	OC-48
9953.28 Mbps	STS-192	STM-64	OC-192

Table 1. Common SONET/SDH Rates (After Ref. [3].)

2. Overhead Bytes

The SONET definitions of some overhead messages are more tuned to the operating conditions within North America, while the SDH equivalents are more general in nature.

This tuning of overhead messages are needed as both the SONET and SDH use different terms to describe the three layers of network topology. SONET uses the terms path, line and section while SDH uses the terms path, multiplex section and regenerator section, as shown in Figures 1 and 2 below.

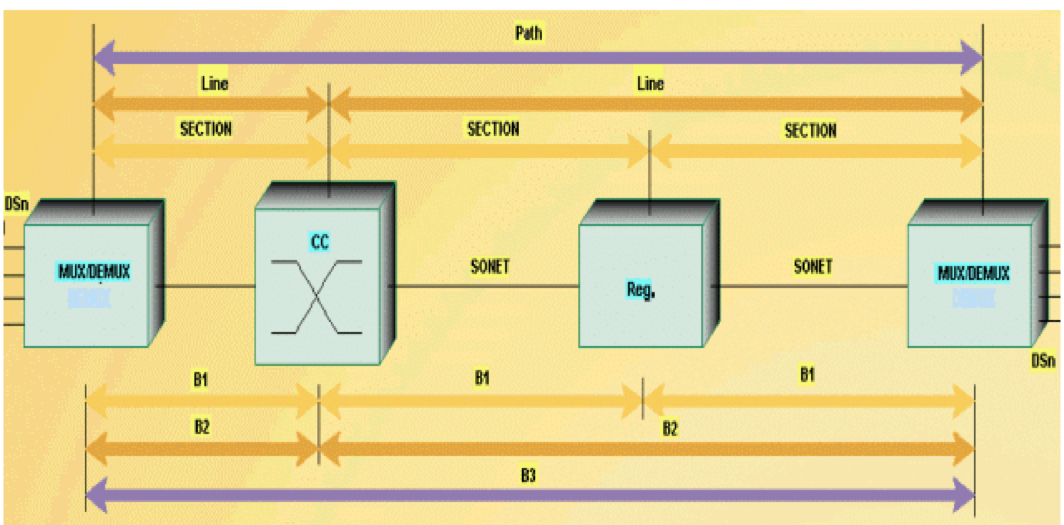

Figure 1. SONET Link (From Ref. [4].)

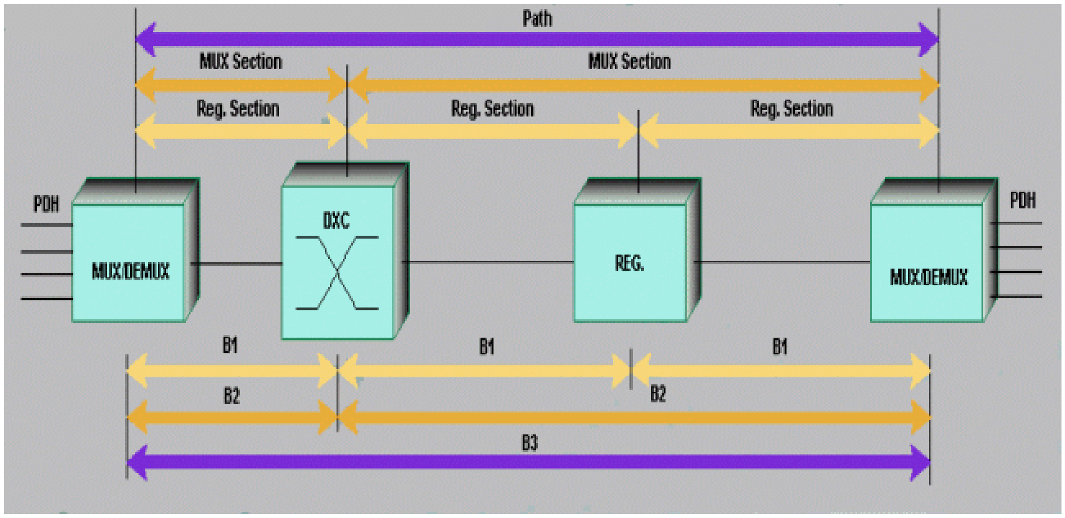

Figure 2. SDH Link (From Ref. [4].)

As for specific overhead bytes, the content of Automatic Protection Systems (APS) messages transmitted in the K1/K2 bytes and the values of the C2 Path Overhead (POH) byte are slightly different for SDH as compared to SONET as the frame structures between the two are different as shown in Figures 3 and 4 below.

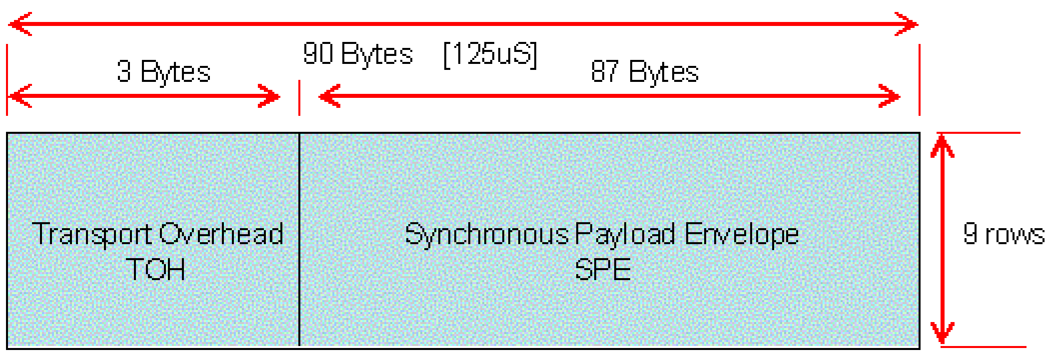

Figure 3. SONET Frame Structure (From Ref. [3].)

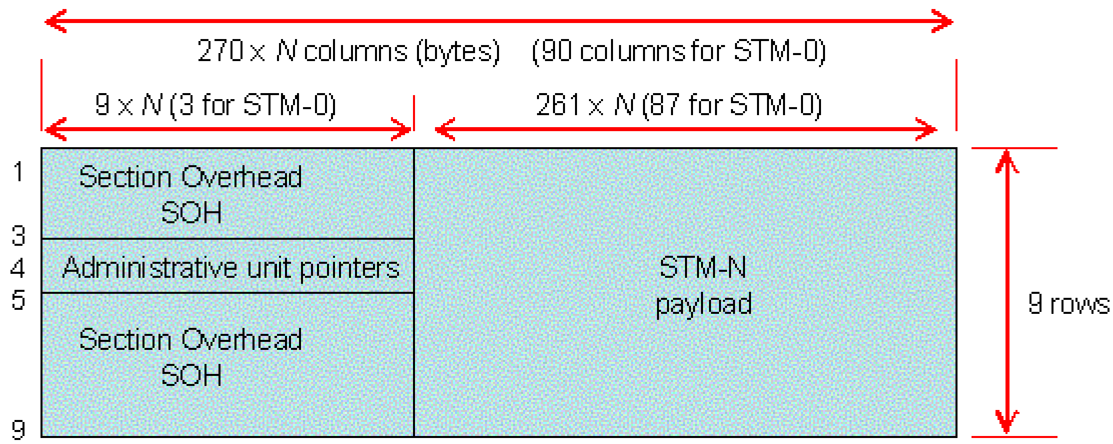

Figure 4. STM-N Frame Structure (From Ref. [3].)

E. SUMMARY

This chapter reviewed the evolution of Synchronous Optical Network (SONET) / Synchronous Digital Hierarchy (SDH) from a relatively unknown technology to become widely deployed in the Telecommunications Industries. Some of the advantages and usefulness of SONET/SDH are discussed. The main differences between SONET and SDH are also presented.

In the next chapter, we will look at the basic configuration of a simple SONET network and the SONET architecture.

III. ARCHITECTURE

A. CHAPTER OVERVIEW

In this chapter, we will look at the basic configuration of a simple SONET network and the terminologies that defines the equipment. After which, we will drill into the SONET architecture, explain a bit on the multiplexing hierarchy, its frame structure, functions of the overhead bytes, and how are they are being used in the SONET built-in standards for Operations, Administration, Maintenance and Provisioning (OAM&P).

B. BASIC CONFIGURATION

A very simple SONET network could consist of two terminals with a length of fiber between them. If the distance is too long for one fiber link, *regenerators* are used to amplify and reconstruct the physical signal. An *add/drop multiplexer* provides two fiber connections with the ability to access the internal structure of the SONET frame to remove or insert individual channels as required for that node while passing the rest of the traffic on through. Digital Cross-connects (DXC) are used to switch, combine, redirect, and otherwise groom traffic, with varying degrees of granularity. All of these elements are *section terminating equipment*; all except regenerators are also *line terminating equipment*. Network elements where non-SONET signals are attached to the SONET network are *path terminating equipment*. All elements are intelligent, accessing in-band management information dedicated to each layer within the SONET frame [1].

Figure 5 shows a typical SONET connection.

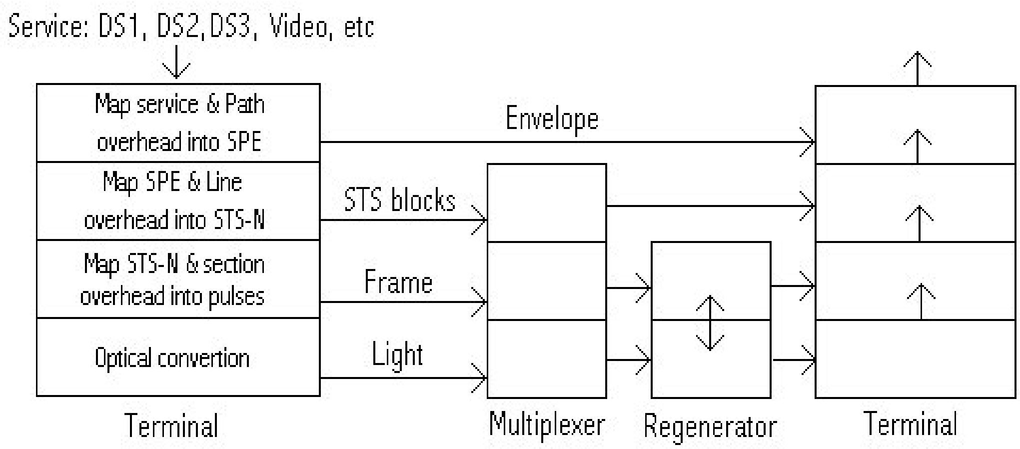

Figure 5. Typical SONET Connection (From Ref. [5].)

Within metropolitan areas, SONET networks are typically configured physically as rings, as shown in Figure 6 below. A ring topology provides a single level of redundancy, allowing restoration of service if one fiber link is broken. The SONET mechanism for restoration takes less than 50 milliseconds to recover from a break, but is considered somewhat inefficient as half the total ring bandwidth is reserved [1]. Note that even though the physical topology may be a ring, the individual channels (which are manually provisioned) are point-to-point — SONET has no equivalent of Ethernet/IP broadcast or multicast service [1].

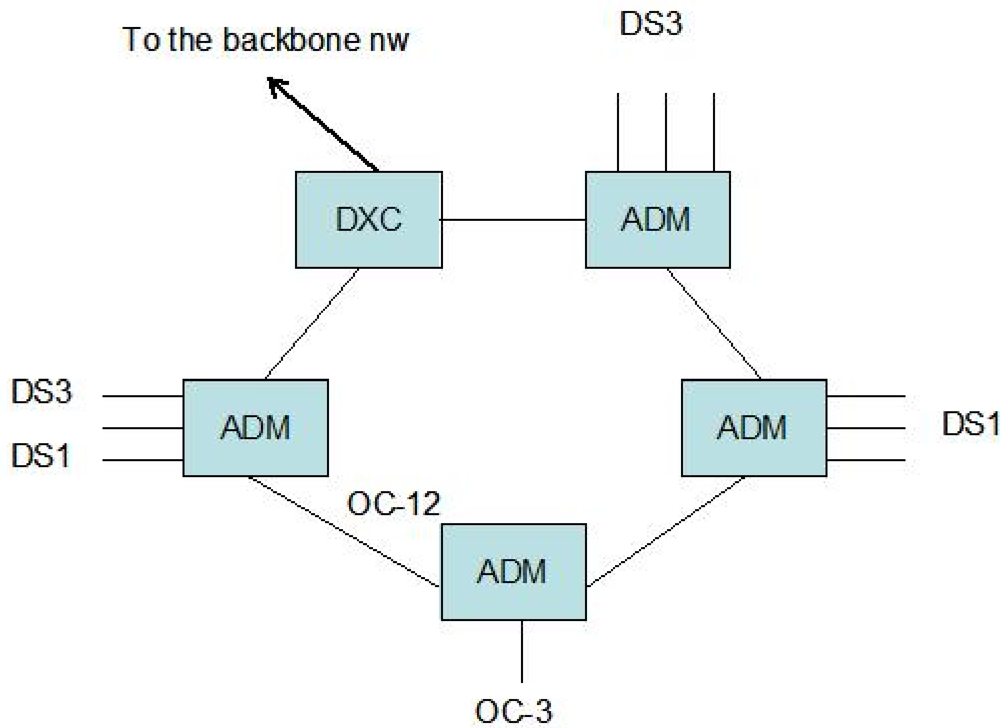

Figure 6. An example of a SONET Ring configuration (After Ref. [1].)

C. MULTIPLEXING HIERARCHY

The STS-1 frame is described as an array of bytes 90 columns wide by nine rows high. This works out to be 810 bytes or 6480 bits per frame transmitted every 125us, or at a rate of 8,000 frames per second. This results in a basic SONET signal rate of 51.840 Mbit/sec (8000 fps * 810 b/frame), of which the payload is roughly 49.5 Mbps, enough to encapsulate 28 DS-1s, a full DS-3 or 21 CEPT-1s. All higher level signals are multiples of this rate.

An STS-3 is very similar to STS-3c. The frame is 9 rows by 270 bytes. The first 9 columns contain the transport overhead section and the rest is for the Synchronous Payload Envelope (SPE). The transport overhead (Line and Section) is the same for both STS-3 and STS-3c.

For an STS-3 frame, the SPE contains 3 separate payloads and 3 separate path overhead fields. In essence, it is the SPE of three separate STS-1's packed together one after the other.

In STS-3c, there is only one path overhead field for the entire SPE. The SPE for an STS-3c is a much larger version of a single STS-1 SPE.

Figure 7 shows the SONET Multiplexing Hierarchy.

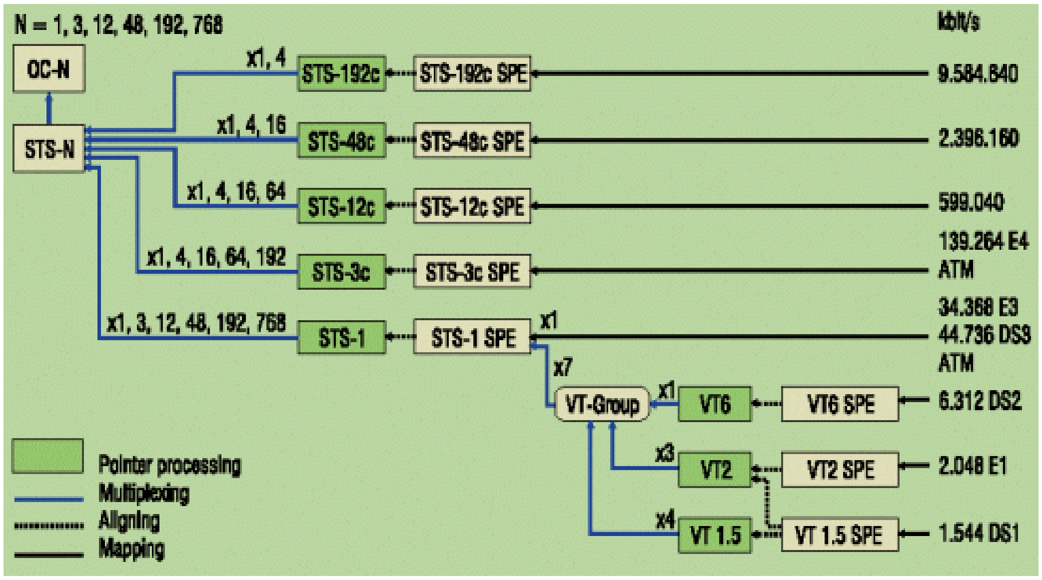

Figure 7. SONET Multiplexing Hierarchy (From Ref. [4].)

D. FRAME STRUCTURE

The most basic element of the Synchronous Optical Network (SONET) standards is the synchronous transport signal level 1 (STS-1), which provides the framing for transmission of control information along with the customer traffic [5]. This frame format is used for all SONET transmissions. As the data rates increase, more copies of the STS-1 frame are transmitted for each transmission period. Unlike Ethernet or IP where the frame structure is usually illustrated linearly, the large frame sizes involved in SONET are depicted as two dimensional matrices.

As stated above, a standard STS-1 frame is 9 rows by 90 bytes as shown in Figure 8. The figure is read left to right, then top to bottom. The first 3 bytes of each row comprise the Section and Line overhead. These overhead bits are comprised of framing bits, and pointers to different parts of the SONET frame.

The combination of the Section and Line overhead comprises the "Transport Overhead". The transport overhead carries the section and line overhead control information, including parity, trace, alarm signals, orderwire, and data communication channels (DCC).

There is one column of bytes in the payload that comprises the STS path overhead. This column frequently "floats" throughout the frame. Its location in the frame is determined by a pointer in the Section and Line overhead.

The remainder is the Synchronous Payload Envelope (SPE). The SPE carries the information that must traverse the entry and exit points through the SONET network. This information includes both the payload traffic and the path overhead. The path overhead coordinates the activities between the SONET terminals (or add/drop multiplexers) that are responsible for the entry and exit points through the network.

Figure 8 shows the Synchronous Transport Signal level 1 (STS-1) frame structure.

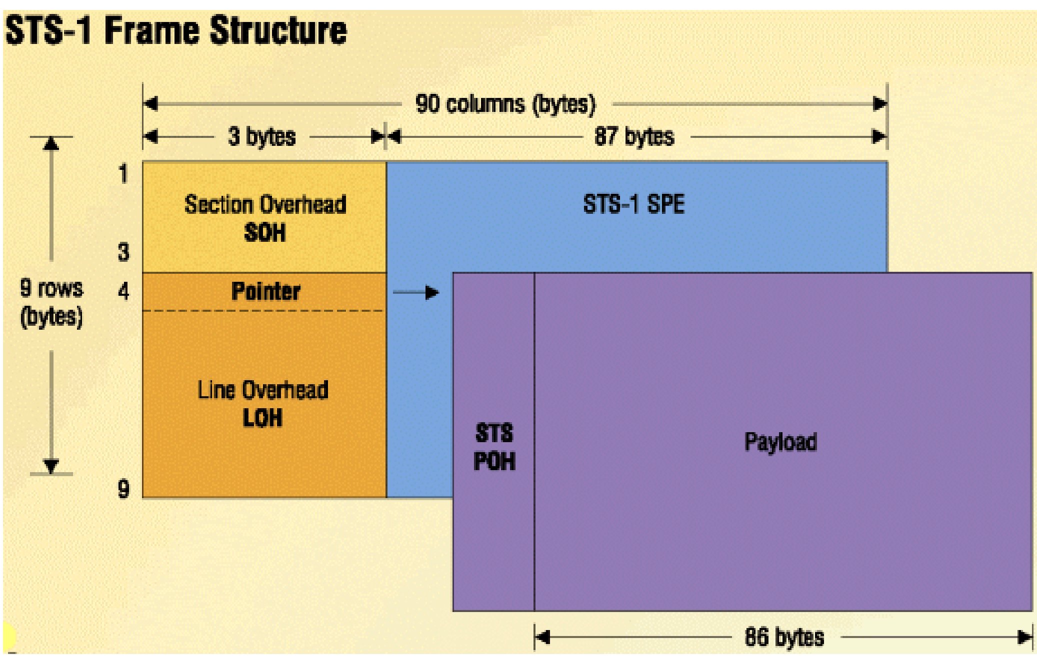

Figure 8. STS-1 Frame Structure (From Ref. [4].)

E. OVERHEAD TYPES

Figure 9 shows the STS-1 Transport and Path Overhead (SONET Overhead).

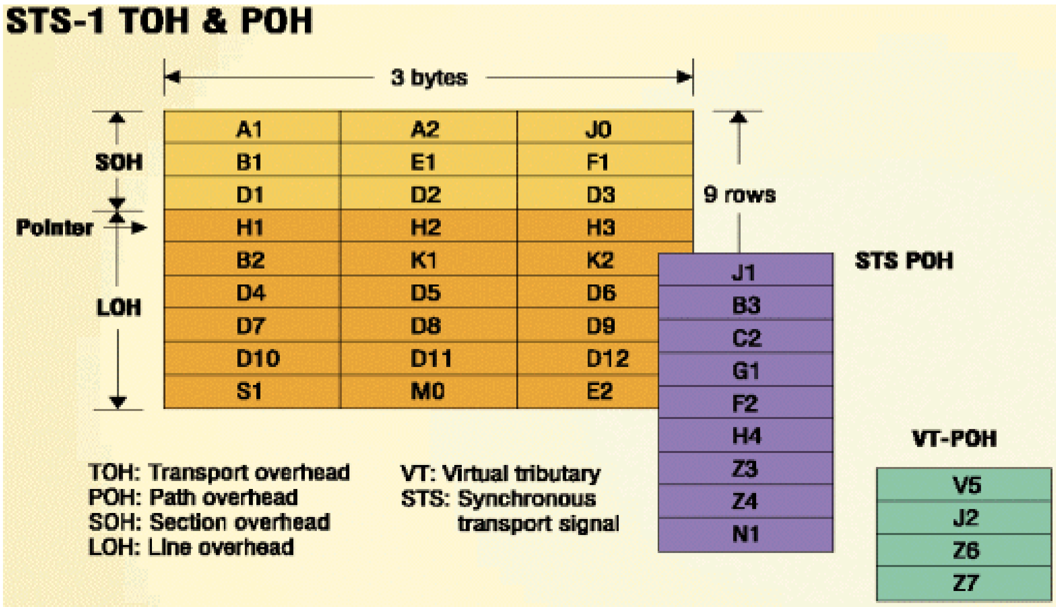

Figure 9. STS-1 TOH & POH (From Ref. [4].)

1. Transport Overhead

The transport overhead, which is shown in Table 2, provides mechanisms to control the section and line interactions over the SONET network. At the lowest logical level, the section interactions provide for the physical link between adjacent peer equipment, such as the transfer of information between a SONET terminal and a regenerator.

Transport Overhead			
Section overhead	Framing A1	Framing A2	Trace/growth (STS-ID) J0/Z0
	BIP-8 B1/undefined	Orderwire E1/undefined	User F1/undefined
	Data comm D1/undefined	Data comm D2/undefined	Data comm D3/undefined
Line overhead	Pointer H1	Pointer H2	Pointer action H3
	BIP-8 B2	APS K1/undefined	APS K2/undefined
	Data comm D4/undefined	Data comm D5/undefined	Data comm D6/undefined
	Data comm D7/undefined	Data comm D8/undefined	Data comm D9/undefined
	Data comm D10/undefined	Data comm D11/undefined	Data comm D12/undefined
	Sync status/growth S1/Z1	REI-L/growth M0 or M1/Z2	Orderwire E2/undefined

Table 2. Transport Overhead (After Ref. [6].)

2. Section Overhead (SOH)

The section overhead information manages the transport of the optical channel information between adjacent SONET equipment (at each end of a fiber), roughly corresponding to the OSI link layer. Services mapped to the

section overhead include framing, channel trace, performance monitoring, voice orderwire, and an overlay data communications channel (DCC).

Figure 10 provides a description of all the bytes from STS-1 Section Overhead (SOH).

SOH Section Overhead

A1, A2: Indicates the beginning of each STS-1 within a STS-n frame. The pattern is Hex F628.

J0: Section trace. It is defined only for STS-1 number 1 of an STS-N signal. Used to transmit a one byte fixed length string or a 16 byte message so that a receiving terminal in a section can verify its continued connection to the intended transmitter.

Z0: Section growth. It is defined in each STS-1 for future growth except for STS-1 number 1 (which is defined as J0).

B1: Section error monitoring. The BIP-8 is calculated over all bits of the previous STS-N frame after scrambling and is placed in the B1 byte of STS-1 number 1 before scrambling. Defined only for STS-1 number 1 of an STS-N signal.

E1: Allocated to be used as local orderwire channels for voice communication between section terminating equipments, hubs and remote terminal locations.

F1: Reserved for user purposes (e.g. temporary data/voice channel connections for special maintenance purposes).

D1 - D3: Data communication channels (DCC). A 192 kbit/s message based channel for alarms, maintenance, control, monitoring, administration and other communication needs.

Figure 10. Descriptions of STS-1 SOH (From Ref. [4].)

3. Line Overhead (LOH)

Where the section overhead provides a set of mechanisms to coordinate the point-to-point transmission of information, the line overhead services concentrate on the alignment and delivery of information between terminals and add/drop multiplexing equipment. The line overhead also defines data channels carrying Operations, Administration, Maintenance and Provisioning (OAM&P) information, which would be application layer information (like SNMP) in an OSI modeled network.

Figures 11 and 12 provide a description of all the bytes from STS-1 Line Overhead (LOH).

LOH Line Overhead

H1, H2: Pointer bytes. Allocated to a pointer that indicates the offset in bytes between pointer and the first byte of the STS SPE. It is used to align the STS-1 transport overheads in an STS-N signal as well as perform frequency justification.

H3: Pointer action byte. It is used for frequency justification. Depending on the pointer value, this byte is used to adjust the fill input buffers. It only carries valid information in the event of negative justification, otherwise it's not defined.

B2: Line error monitoring. The BIP-8 is used to determine if a transmission error has occurred over a line. It is calculated over all bits of the previous STS-1 frame before scrambling and is placed in the B2 byte of the current frame before scrambling.

K1, K2: Allocated for APS (Automatic Protection Switching) signaling for the protection of the multiplex section.

Linear APS messages

ANSI T1.105.01 protection switching protocol	
K1 byte	**Condition**
b1 - b4	
1111	Lockout of protection
1110	Forced switch
1101	Signal fail high priority
1100	Signal fail low priority
1011	Signal degrade high priority
1010	Signal degrade low priority
1001	Unused
1000	Manual switch
0111	Unused
0110	Wait-to-restore
0101	Unused
0100	Exercise
0011	Unused
0010	Reserve request
0001	Do not revert
0000	No request
b5 - b8	Selects channel used by APS messages
K2 byte	**Condition**
b1 - b4	Selects bridged channel used
b5	Determines automatic protection switch architecture
b6 - b8	000 = Reserved for future use 001 = Reserved for future use 010 = Reserved for future use 011 = Reserved for future use 100 = Reserved for future use 101 = Reserved for future use 110 = MS-RDI 111 = MS-AIS

Ring APS messages

ANSI T1.105.01 protection switching protocol	
K1 byte	**Condition**
b1 - b4	
1111	Lockout of protection (span) or signal fail (protection)
1110	Forced switch (span)
1101	Forced switch (ring)
1100	Signal fail (span)
1011	Signal fail (ring)
1010	Signal degrade (protection)
1001	Signal degrade (span)
1000	Signal degrade (ring)
0111	Manual switch (span)
0110	Manual switch (ring)
0101	Wait-to-restore
0100	Exerciser (span)
0011	Exerciser (ring)
0010	Reserve request (span)
0001	Reserve request (ring)
0000	No request
b5 - b8	Destination node ID
K2 byte	**Condition**
b1 - b4	Source node ID
b5	Path code: 0 = short path; 1 = long path
b6 - b8	000 = Idle 001 = Bridged 010 = Bridged and switched 011 = Reserved for future use 100 = Reserved for future use 101 = Reserved for future use 110 = MS-RDI

Figure 11. Descriptions of STS-1 LOH (from [4].)

D4 - D12: Data Communication Channels (DCC). These 9 bytes form a 576 kbit/s message channel for alarms, maintenance, control, monitor, administration and other communication needs between line-terminating entities.

S1: Synchronization messaging. Bits 5 - 8 are used to carry the synchronization status messages which provide an indication of the quality level of the synchronization source of the SONET signal. Bits 1 - 4 are reserved for future use.

SONET Synchronization Status Messages

S1 byte b5 - b8	SONET synchronization quality level description
0000	Synchronized-traceability unknown
0001	Stratum 1 traceable
0111	Stratum 2 traceable
1010	Stratum 3 traceable
1100	±20 ppm clock traceable
1110	Reserved for network synchronization
1111	Don't use for synchronization

M0: Only defined for STS-1 signal. Bits 5 - 8 are used as a line REI function. They convey the count of errors detected by B2. Bits 1 - 4 are reserved for future use.

M1: This byte is located in the third STS-1 in order of appearance in the byte interleaved STS-N frame and is used as a line REI function. It conveys the count of errors detected by B2.

Z1: In SONET signals and at rates above STS-1 and below STS-192, this byte is defined in each STS-1 number 1 for future growth.

Z2: In SONET signals and at rates above STS-1 and below STS-192, this byte is defined in each STS-1 except the third STS-1 for future growth.

E2: Allocated for an express orderwire between line entities. It is defined only for STS-1 number 1 of an STS-N signal and its use is optional.

Figure 12. STS-1 LOH descriptions continued (From Ref. [4].)

4. Path Overhead (POH)

With the line and section services providing the mechanisms needed to frame and deliver the STS-1 frames, the SPE contains a combination of path overhead and payload traffic. The path overhead is the end-to-end transport of a circuit, which also has application information (performance monitoring, status, tracing) for management.

Table 3 and Figures 13 and 14 provide a description of all the bytes from STS-1 Path Overhead (POH).

Path Overhead
J1 - Trace
B3 – Error Monitor
C2 – Signal label
G1 – Status
F2 – Users Channel
H4 – Multi Frame Indicator
Z3 – Future use
Z4 – Future Use
N1 – Tandem Connection

Table 3. Path Overhead (After Ref. [6].)

STS POH STS Path Overhead

J1: STS path trace. It is used to transmit a 64-byte, fixed-length string so that a receiving terminal can verify its continued connection to the intended transmitter.

B3: Path error monitoring. The BIP-8 is calculated over all bits of the previous STS SPE before scrambling. Computed value is placed in the B3 byte.

C2: Signal label. Allocated to identify the construction and content of the STS-level SPE and for PDI-P.

C2 byte coding

Code [hex]	Payload type
00	Unequipped
01	Equipped – nonspecific
02	Floating VT mode
03	Locked VT mode
04	Asynchronous mapping for DS3
12	Asynchronous mapping for 139.264 Mbit/s
13	Mapping for ATM
14	Mapping for DQDB
15	Asynchronous mapping for FDDI
16	Mapping for HDLC over SONET
E1	STS-1 payload with 1 VT-x payload defect
E2	STS-1 payload with 2 VT-x payload defects
E3	STS-1 payload with 3 VT-x payload defects
E4	STS-1 payload with 4 VT-x payload defects
E5	STS-1 payload with 5 VT-x payload defects
E6	STS-1 payload with 6 VT-x payload defects
E7	STS-1 payload with 7 VT-x payload defects
E8	STS-1 payload with 8 VT-x payload defects
E9	STS-1 payload with 9 VT-x payload defects
EA	STS-1 payload with 10 VT-x payload defects
EB	STS-1 payload with 11 VT-x payload defects
EC	STS-1 payload with 12 VT-x payload defects
ED	STS-1 payload with 13 VT-x payload defects
EE	STS-1 payload with 14 VT-x payload defects
EF	STS-1 payload with 15 VT-x payload defects
F0	STS-1 payload with 16 VT-x payload defects
F1	STS-1 payload with 17 VT-x payload defects
F2	STS-1 payload with 18 VT-x payload defects
F3	STS-1 payload with 19 VT-x payload defects
F4	STS-1 payload with 20 VT-x payload defects
F5	STS-1 payload with 21 VT-x payload defects
F6	STS-1 payload with 22 VT-x payload defects
F7	STS-1 payload with 23 VT-x payload defects
F8	STS-1 payload with 24 VT-x payload defects
F9	STS-1 payload with 25 VT-x payload defects
FA	STS-1 payload with 26 VT-x payload defects
FB	STS-1 payload with 27 VT-x payload defects
FC	STS-1 payload with 28 VT-x payload defects, or STS-1, STS-3c, etc. with a non-VT payload defect (DS3, FDDI, etc.)

G1: Path status. Allocated to convey back to an originating STS SPE the path-terminating status and performance. Bits 1 - 4 convey the count of interleaved bit blocks that have been detected in error by B3. Bits 5 - 7 provide codes to indicate both an old version and an enhanced version of the STS RDI-P.

Figure 13. Description of STS-1 POH (From Ref. [4].)

G1, RDI-P defects

REI				RDI-P			Spare
b1	b2	b3	b4	b5	b6	b7	b8

b5	b6	b7	Interpretation	Triggers
0	0	0	No remote defect	No defects
0	0	1	No remote defect	No defects
0	1	0	Remote payload defect	PLM-P
0	1	1	No remote defect	No defects
1	0	0	Remote defect	AIS-P, LOP-P
1	0	1	Remote server defect	AIS-P, LOP-P
1	1	0	Remote connectivity defect	TIM-P, UNEQ-P
1	1	1	Remote defect	AIS-P, LOP-P

F2: Path user channel. Allocated for user communication purposes between path elements.

H4: Multiframe indicator. Provides a generalized multiframe indicator for payloads. Currently, it is only used for VT-structured payloads.

Z3, Z4: Allocated for future use. Have no defined value. The receiver is required to ignore their content.

N1: Allocated to support tandem connection maintenance and the tandem connection link. Bits 1 - 4 are used to provide the tandem connection Incoming Error Count (IEC). In option 1, bits 5 - 8 are used to provide the tandem connection data link which is an optional 32 kbit/s data channel available to applications or services that span more than one LTE-LTE connection, but may be shorter than a PTE-PTE connection. In option 2, bits 5 - 8 are used to provide maintenance information including REI, outgoing error indication, RDI, outgoing defect information and TC access point identifier.

Figure 14. STS-1 POH description continued (From Ref. [4].)

5. Virtual Tributary Line Overhead (VT POH)

As its name implies, the VT-POH is the virtual end-to-end transport of a circuit, which also has application information (performance monitoring, status, tracing) for management.

Figure 15 provides a description of all the bytes from STS-1 Virtual Tributary Path Overhead (VT POH).

VT-POH VT Path Overhead

(for VT-1.5, VT-2, VT-3, VT-6)

V5: The first byte of a VT SPE, provides the functions of error checking, signal label and path status. Bits 1 and 2 are allocated for error performance monitoring. Bit 3 is a REI-V that is sent back towards an originating VT PTE if errors were detected by the BIP-2. Bit 4 is reserved for mapping-specific functions. Bits 5 - 7 provide a VT signal label. Bit 8 provides codes to indicate both an old version and an enhanced version of the RDI-V.

b5 - b7	Assigned VT Identification
000	Unequipped VT1.5
001	Equipped – nonspecific VT1.5
010	Asynchronous mapping for DS1
011	Bit-synchronous mapping for DS1
100	Byte synchronous mapping for DS1
101	Unassigned VT1.5
110	Unassigned VT1.5
111	Unassigned VT1.5
000	Unequipped VT2
001	Equipped – nonspecific VT2
010	Asynchronous mapping for 2.048 Mbit/s
011	Bit-synchronous mapping for 2.048 Mbit/s
100	Byte synchronous mapping for 2.048 Mbit/s
101	Unassigned VT2
110	Unassigned VT2
111	Unassigned VT2
000	Unequipped VT3
001	Equipped – nonspecific VT2
010	Asynchronous mapping for 2.048 Mbit/s
011	Bit-synchronous mapping for 2.048 Mbit/s
100	Byte synchronous mapping for 2.048 Mbit/s
101	Unassigned VT2
110	Unassigned VT2
111	Unassigned VT2
000	Unequipped VT3
001	Equipped – nonspecific VT3
010	Asynchronous mapping for DS1C
011	Unassigned VT3
100	Unassigned VT3
101	Unassigned VT3
110	Unassigned VT3
111	Unassigned VT3
000	Unequipped VT6
001	Equipped – nonspecific VT6
010	Asynchronous mapping for DS2
011	Unassigned VT6
100	Unassigned VT6
101	Unassigned VT6
110	Unassigned VT6
111	Unassigned VT6

Figure 15. Description of STS-1 VT-POH (From Ref. [4].)

F. OAM&P

One of the important features of SONET/SDH is its built-in standards for Operations, Administration, Maintenance and Provisioning (OAM&P). It covers all the major day-to-day operations and fault detections in the SONET/SDH network.

Listed below are the overhead bytes that are directly related to the SONET OAM&P. Their detailed description and usage were provided in earlier this section.

1. A1/A2 Framing bytes
2. D1, D2 and D3 DCC bytes
3. H1/H2 Pointer bytes
4. K1/K2 Automatic Protection Switching (APS) bytes
5. D4 – D12 DCC bytes
6. S1 Synchronization byte
7. M0/M1 byte
8. C2 Signal Path byte
9. G1 path Status Byte

Figure 16 presents an overview of how the various OAM&P overhead bytes are used and interacted.

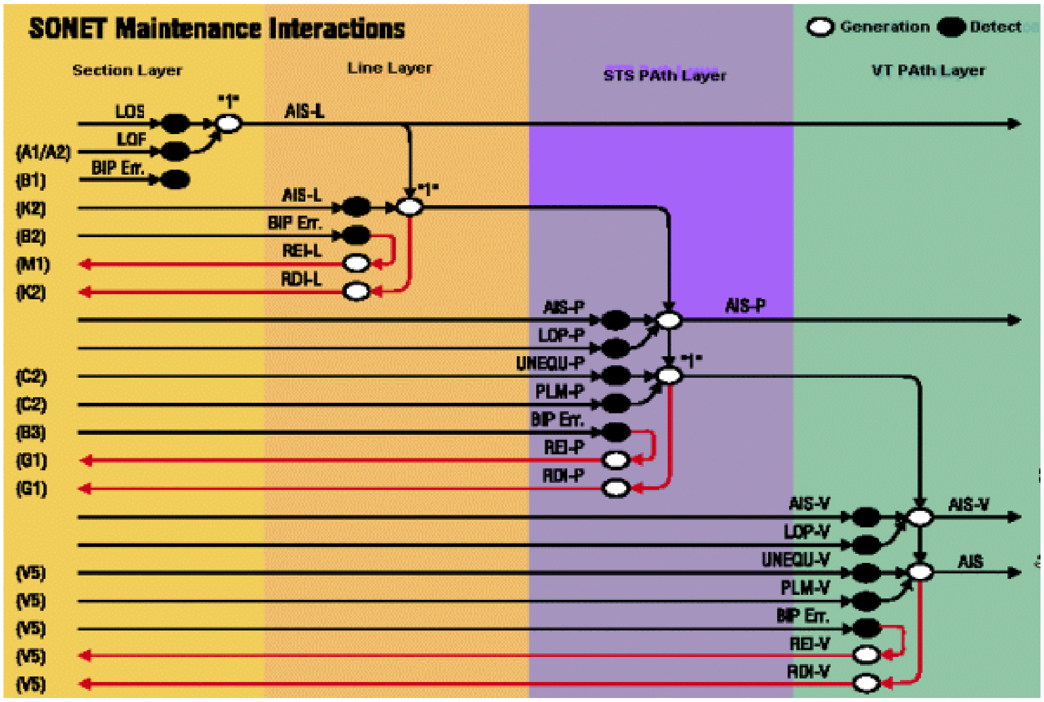

Figure 16. SONET Maintenance Interactions (From Ref. [4].)

SONET/SDH standards define various major failure conditions and their associated alarm indicators. They are used to inform the SONET/SDH network where failure exists. Figure 17 lists the major failures, what the alarms mean and their detection criteria.

	Anomalies / Defects	Detection criteria	Bellcore ANSI
LOS	Loss of Signal	All-zero pattern for 2.3 $\mu s \le T \le 100\ \mu s$	GR-253 T1.231
SEF	Severely Error Framing	A1, A2 errored for $\ge 625\ \mu s$	GR-253 T1.231
LOF	Loss of Frame	If SEF persists for ≥ 3 ms	GR-253 T1.231
S-BIP Error	Section BIP Error (B1)	Mismatch of the recovered and computed BIP-8 covers the whole STS-N frame	GR-253 T1.105
L-BIP Error	Line BIP Error (B2)	Mismatch of the recovered and computed N x BIP-8 covers the whole frame, except section overhead	GR-253 T1.105
AIS-L	Line-AIS	K2 (bits 6, 7, 8) = 111 for ≥ 5 frames	GR-253 T1.231
REI-L	Line Remote Error Indication	Number of detected B2 errors in the sink side encoded in byte M0 or M1 of the source side	GR-253 T1.105
RDI-L	Line Remote Defect Indication	K2 (bits 6, 7, 8) = 110 for $\ge z$ frames ($z = 5 - 10$)	GR-253 T1.231
AIS-P	STS Path AIS	All "1" in the STS pointer bytes H1, H2 for ≥ 3 frames	GR-253 T1.231
LOP-P	STS Path Loss of Pointer	8 - 10 NDF enable 8 - 10 invalid pointers	GR-253 T1.231
P-BIP Error	STS Path BIP Error (B3)	Mismatch of the recovered and computed BIP-8 covers entire STS-SPE	GR-253 T1.105
UNEQ-P	STS Path Unequipped	C2 = "0" for ≥ 5 (≥ 3 as per T1.231) frames	GR-253 T1.231
TIM-P	STS Path Trace Identifier Mismatch	Mismatch of the accepted and expected Trace Identifier in byte J1 (64 bytes sequence)	GR-253 T1.105
REI-P	STS Path Remote Error Indication	Number of detected B3 errors in the sink side encoded in byte G1 (bits 1, 2, 3, 4) of the source side	GR-253 T1.105
RDI-P	STS Path Remote Defect Indication	G1 (bit 5) = 1 for ≥ 10 frames	GR-253 T1.231
PLM-P	STS Path Payload Label Mismatch	Mismatch of the accepted and expected Payload Label in byte C2 for ≥ 5 (≥ 3 as per T1.231) frames	GR-253 T1.231
LOM	Loss of Multiframe	Loss of synchronization on H4 (bits 7, 8) superframe sequence	GR-253 T1.105
AIS-V	VT Path AIS	All "1" in the VT pointer bytes V1, V2 for ≥ 3 superframes	GR-253 T1.231
LOP-V	VT Loss of Pointer	8 - 10 NDF enable 8 - 10 invalid pointers	GR-253 T1.231
V-BIP Error	VT Path BIP Error (BIP-2)	Mismatch of the recovered and computed BIP-2 (V5 bits 1, 2) covers entire VT	GR-253 T1.105
UNEQ-P	VT Path Unequipped	V5 (bits 5, 6, 7) = 000 for ≥ 5 (≥ 3 as per T1.231) superframes	GR-253 T1.231
TIM-V	VT Path Trace Identifier Mismatch	Mismatch of the accepted and expected Trace Identifier in byte J2	for further study
REI-V	VT Path Remote Error Indication	If one or more BIP-2 errors detected in the sink side, byte V5 (bits 3) = 1 on the source side	GR-253 T1.105
RDI-V	VT Path Remote Defect Indication	V5 (bit 8) = 1 for ≥ 10 superframes	GR-253 T1.231
PLM-V	VT Path Payload Label Mismatch	Mismatch of the accepted and expected Payload Label in byte V5 (bits 5, 6, 7) for ≥ 5 (≥ 3 as per T1.231) superframes	GR-253 T1.231

Figure 17. Major Alarm Indicators in OAM&P (From Ref. [4].)

G. SUMMARY

This chapter gives us an understanding of the basic configuration of a simple SONET network and the terminologies used. The SONET architecture on the multiplexing hierarchy, its frame structure, functions of the overhead bytes were also explained.

In the next chapter, we will look at the Data Communications Channel (DCC), Data Communications Network (DCN) and the main features and new updates available in the ITU-T G.7712 standard.

IV. THE DCC, DCN & THEIR STANDARDS

A. CHAPTER OVERVIEW

In this chapter, we will look at the definitions and usage of Data Communications Channel (DCC) and Data Communications Network (DCN). Then we explore the two main protocols used by the network management of SONET/SDH, the OSI and SNMP (IP). We then explain why there is a push for IP over the DCC before completing the chapter with a discussion of the main features and new updates available in the ITU-T G.7712 standard.

B. DCC & DCN

The DCC is 12-bytes long and can be found in the SOH and LOH. In the section layer, three bytes (D1-D3) are allocated in STS-1, the lowest level of an STS-N signal for section data communications. These three bytes are treated as one 192 kbps data channel for the transmission of alarms, maintenance, control, monitor, administration as well as other network element communication needs. In the line layer, 9 bytes (D4-D12) are used as a 576 kbps data channel for similar purposes. Use of the LOH for DCC traffic provides a large pipe and allows for the delivery of more information using the overhead channel [7].

The DCN is a data network that supports layer 1 (physical), layer 2 (data-link), and layer 3 (network) functionalities and consists of routing/switching functionality interconnected via links. It is also designed to support the transportation of distributed Management Communications Network (MCN) and Signaling Communications Network (SCN) for Telecommunications Management Networks (TMN) and Automatic Switched Transport Networks (ASTN) respectively [8].

A typical SONET Network management communications architecture utilizing the Section DCC is shown in Figure 18. Briefly, one or more Operations Systems (OSs) manages the Network Elements (NEs). Connectivity between the OS and NEs is achieved through a Data Communications Network (DCN).

An NE which directly attaches to the DCN is referred to as a Gateway NE (GNE). Access to NEs subtending off the GNE is achieved through the Embedded Operations Channel (EOC) which in the case of SONET is the Section DCC.

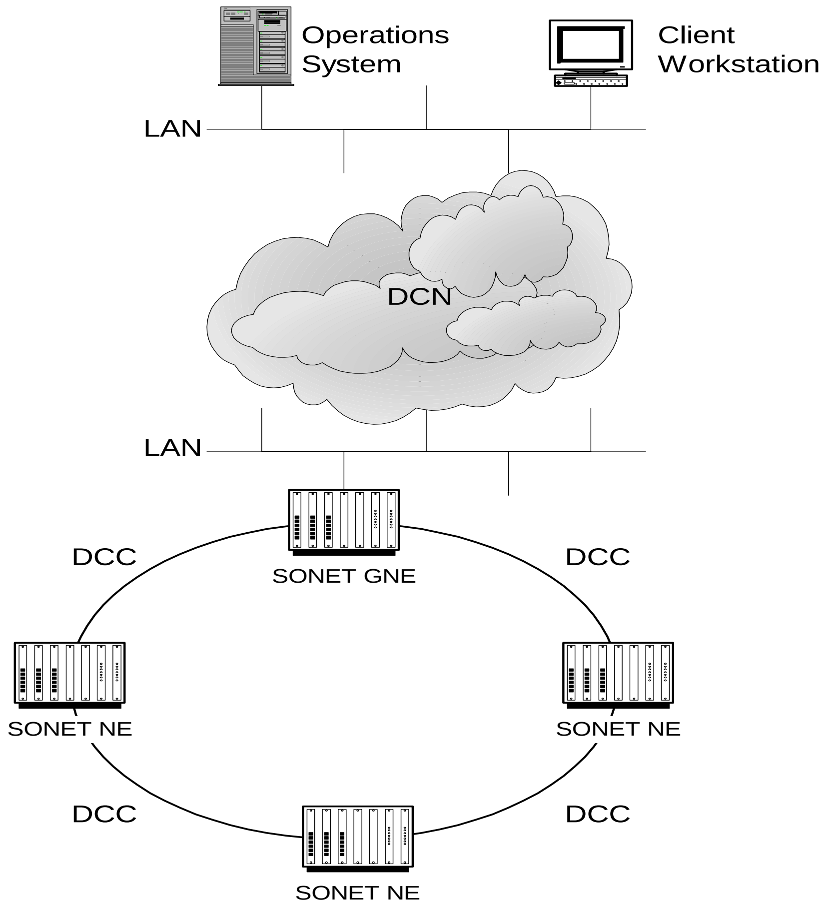

Figure 18. Typical SONET Network Management Communication Architecture (From Ref. [9].)

C. OSI

OSI network management is consistent with the overall OSI application layer architecture. The SONET standards specify a 7-layer OSI protocol stack for both the DCN and the SONET Section DCC. OSI was selected as the standard, because OSI protocols were accepted as the basis for the larger set of Telecommunications Management Network (TMN) standards. CMISE is specified at the application layer (layer 7) for the management of SONET Network Elements (NEs).

Besides defining the managed objects (MIB), the Common Management Interface Services Elements (CMISE) standard [10] also defined several system management functions (SMFs) to support the more generalized System Management Functional Areas (SMFAs) such as fault, configuration, accounting, performance and security management.

Some of the standardized SMFs include [10]:

1. Object management
2. State management
3. Relationship management
4. Alarm reporting
5. Event management
6. Log control
7. Security alarm reporting
8. Confidence and diagnostic testing
9. Summarization function
10. Workload monitoring function

OSI network management is quite comprehensive but complex as compared to SNMP. However, the OSI vision for the TMN though has been difficult to achieve. CMISE saw only modest deployment for managing SONET equipment, while the vast majority of products continued to be managed with Transaction Language 1 (TL1). TL1 is a traditional telecom language for managing and reconfiguring SONET network elements. TL1 over OSI gave rise to the TARP protocol, which permits resolutions of an OSI Network Service Access Point (NSAP) address from a TL1 Target Identifier (TID) and vice versa. NSAP is the information that the OSI Network service provider needs to identify a particular network element whereas TID is a unique name given to each system when it is installed. The name identifies the particular NE, to which each command is directed.

D. SNMP

Compared to OSI, the SNMP layers are much simpler than the OSI suite. In SNMP, the network management applications consist of vendor-specific modules such as fault management, log control, security and audit trails but there are no real standards or specifications defined. The interactions of the SNMP

layers with respect to the SONET/SDH are similar but simpler than the OSI sequence. Basically, management applications map the SNMP management traffic instead of OSI headers into the DCC fields or the payload areas for onward transmission to the management process.

Because of the simplicity and similarity of the SNMP network management process, service providers have recently began to request that SONET/SDH products support an IP protocol stack on their OS/NE interface (Ethernet), since many service providers did not want to implement an OSI-based DCN or deploy mediation devices. IP on the OS/NE interface, while leaving OSI on the NE-NE interface (DCC) requires the NE to perform a non-trivial gateway function. The gateway function involves accepting TCP connections on the LAN side, examining the TID of the TL1 message, and setting up an OSI association over the DCC with the remote target NE. The gateway NE also needs to handle file transfers by accepting FTP transfers from the OS to the gateway NE, buffering the file, and then transferring the file to the target NE using the OSI File Transfer Access and Management (FTAM) application protocol.

E. NEED FOR IP OVER DCC

The existing operations communications standards have adequately addressed the traditional SONET network managed using TL1. However, network technology is rapidly advancing to the point where the current standards no longer suffice. The convergence of transport and data communication functionality into a single NE means that TL1 may no longer be sufficient or appropriate as the only management protocol. Data NEs are typically managed with SNMP which poses a problem, since there are no standards addressing how to use SNMP over an OSI-based DCC. As a workaround some vendors have introduced cumbersome IP over OSI tunneling capabilities. Besides SNMP, there are a number of other management protocols which are emerging such as CORBA, HTML, and XML, all of which are transported over IP network. These increasingly important protocols cannot readily be used over an OSI-based DCC, since again the standards only address CMISE and TL1.

Four key areas are highlighted below to address the need for IP over DCC for SONET/SDH network management:

1. Useability

TCP/IP is the common protocol for Data Communication Networks (DCNs). On a larger scale, people are asking as to why there isn't one protocol for the management systems, and because of TCP/IP's momentum, it appears to be the one of choice.

In many cases, OSI requires mediation devices/conversion to be sent over today's DCN.

2. Maintainability

Worldwide acceptance/implementation of TCP/IP provides a large base of subject matter expertise. The IETF is dedicated to supporting TCP/IP protocols for completeness and enhancement work items while the OSI stack's support is dependent on the ISO/ITU-T for creating new standards and for fixing errors in current documents.

The use of OSI protocols in the DCN for DCC integration and interoperation requires the IT professional to also learn the CLNS while maintaining a routed architecture with IP and SNMP. Most IT departments would prefer to manage the IP network for the routers while allowing the operational staff to maintain the OSI portion. Unfortunately, the IT departments must learn both. Most Operational Support Systems (OSS)'s today have an OSI stack and an IP stack. Customers, who would rather run IP at the Network Operation Centre (NOC), and within the DCN, need to provide for a mediation function somewhere before the protocol packet gets to the DCC. Mediation converts the packet from an OSI protocol to a TCP/IP packet. Thus the IT staff is forced to learn both protocols.

An OSS which uses an IP stack forces mediation to OSI at the DCC. To our knowledge the work item for translating FTP to FTAM is incomplete. Hence, no Network and Services Integrated Forum (NSIF) approved standard exists for software download in a mediated DCN.

3. System Cost

OSI generally is purchased for a premium from few remaining OSI stack vendors. The larger OSI stack requires significant system resources, memory and processing.

The use of OSI forces the IT and operations staffs to learn both OSI and TCP/IP since OSI is on the DCC and TCP/IP is used as the maintenance protocol for routers.

4. Prevalance

TCP/IP is the protocol that has become the de-facto standard. It is used in very large developments and has proven velocity in acceptance and services. Applications like HTTP (web), SNMP, and others run on top of TCP/IP; therefore given the huge data explosion, the momentum is definitely with a protocol that supports these applications. OSS & NE's are migrating to Ethernet Interfaces and DCNs have moved from X.25 to IP.

The current direction of the optics standards bodies is to use IP as the protocol of choice for management applications and signaling. This could result in OSI managed SONET technologies surrounded by IP managed topologies, forcing a dual mediation of the protocols if the customer wants to use inband transport for OAM&P — dual by the way of mediation at ingress to the SONET DCC and mediation at the egress off the DCC at the CPE or terminal point.

Old and new OSS systems generally support TCP/IP today. New NEs have come to the market which supports TCP/IP for management transport. The bottom line is there is a tremendous need for an IP over DCC standard. The introduction of a new IP standard will of course create compatibility issues with the embedded base of OSI-based NEs. However, for green field applications (brand-new build) of next generation SONET, hybrid, and optical networks, IP is the clear choice. The problem is the lack of any standard to follow until now, with the birth of the ITU-T G.7712/Y.1203 Standard.

F. ITU-T G.7712/Y.1203 STANDARD

G.7712 is the standard for Architecture and Specification of the Data Communications network (DCN). It will be used for the network management, signaling and routing traffic in SONET/SDH, OTN and DWDM networks [2].

G.7712 is important for the telecommunication industry since it enables intelligent optical networks with combined IP-managed and OSI-managed equipment. It is also crucial for vendors of network edge devices as it allows for easy transport of network management traffic to these devices via the core optical switches without the need to create expensive and complicated overlay networks.

1. Specifications

Two key functional elements are introduced in the G.7712 standard. The first one is the encapsulation of one protocol within another. The other being the Integrated IS-IS protocol for routing IP and CLNP traffics across DCN. Listed in Table 4 below are some of the more important specifications defined in the standard:

a. Data Communication Interworking between Protocols

The standard specifies the lower three layers (Physical, Data-Link and Network Layers) for data communication and any interworking between protocols within the lower three layers are carried out by the Data Communication Function (DCF). The table below shows the protocols supported by the lower three layers:

<table>
<tr><th colspan="4">OSI and IP Protocols</th></tr>
<tr><th></th><th>OSI Model</th><th colspan="2">IP Model</th></tr>
<tr><td>Layer 3 Protocol</td><td>CLNP, IS-IS</td><td colspan="2">IP, OSPF, Integrated IS-IS, BGP</td></tr>
<tr><td>Layer 2 Protocol</td><td>LAPD</td><td>PPP over HDLC</td><td>MAC</td></tr>
<tr><td>Layer 1 Protocol</td><td>ECC</td><td>ECC</td><td>LAN</td></tr>
</table>

Table 4. OSI and IP Protocols supported by SONET/SDH (After Ref. [2].)

The physical layer may be either Ethernet, SDH-DCC (also known as Embedded Control Channel (ECC)), or some timeslot of a PDH signal. Either OSI protocols and TCP/IP protocols build on the same physical layer standards, thus there is no difference between OSI and TCP/IP in this aspect.

The purpose of the data link layer is to provide error free data transmission even on noisy links. This is achieved by framing of data and retransmission of every frame until it is acknowledged from the far end, using flow control mechanisms. Error detection is done by means of error detection codes.

The data link layer in the OSI world makes use of the Q.921 LAPD protocol which must support an information field length of at least 512 octets according to G.784. LAPD is based on HDLC framing.

In the internet world there is no real data link layer protocol, but the subnet protocol which has quite many similarities. The subnet protocol consists of the IMP-IMP protocol which aims to provide a reliable connection between neighbored IMPs.

For Ethernet-based networks, e.g. LANs (Local Area Network), the data link protocol LLC (Logical Link Control) is equally used in OSI and TCP/IP networks.

The network layer provides routing capabilities between source and destination system.

OSI uses the CLNS (Connection Less Network Service) protocols ES-IS for communication of an end system to an intermediate system and IS-IS for communication between intermediate systems.

IP divides messages in datagrams of up to 64k length. Each datagram consists of a header and a text part. Besides some other information, the header contains the source and the destination address of the datagram. IP routes these datagrams through the network using either the Open Shortest Path First (OSPF) protocol or Route Information Protocol (RIP) for path calculation

purposes. However, the service provided by IP is not reliable and the datagrams may be received in the wrong order or they may even get lost in the network.

b. MCN and SCN Data Communication Functions

The DCF shall support the End System (ES) in OSI terms or the Host in IP term functionality. It may also operate as an Intermediate System (IS) in OSI terms or as a router in IP terms. The standard defines all the functions supported when DCF assumed any of the roles mentioned, such as:

(1) ECC Access and Data-Link Termination Function
(2) Ethernet LAN Physical Layer Termination Function
(3) Network Layer PDU into ECC Data-Link / Ethernet Frame Encapsulation Function
(4) Network Layer PDU Forwarding Function
(5) Network Layer PDU Routing Function
(6) Network Layer PDU Interworking Function
(7) Network Layer PDU Encapsulation Function
(8) Network Layer PDU Tunneling Function
(9) IP Routing Interworking Function

c. DCN Functional Architecture

The DCN is aware of the three lower layers protocols and is transparent to the upper layers protocols used by the applications for which it transports. It provides specifications for various data communication functions related to ECC interfaces, Ethernet LAN interfaces, and the network layer capabilities to support either OSI only, IP only or a mixed IP + OSI domains. More importantly, it spelt out the ways to allow automatic encapsulation in a mixed DCN that support different network layer protocols and also ensures backward compatibility with OSI only installed base.

d. LAPD and PPP Encapsulation

The standard defines the encapsulation functions for the network layer PDU into the data-Link frame, be it LAPD or PPP protocols being used in the DCN or via DCC serial links. The HDLC framed signal is a serial bit stream containing stuffed frames surrounded by one or more flag sequences that is used by both LAPD and PPP protocols. The mapping of the HDLC framed signal into the DCC channel is bit-synchronous, not direct mapping of stuffed HDLC frame into bytes within a DCC channel. When carrying only IP over the DCC, PPP in

HDLC framing shall be used as the data-link layer protocol. OSI only interface exist in the network today and LAPD protocol is the data-link layer protocol specified and in use since the beginning. Thus for dual interface to connect to either IP-only or OSI-only interface, the data-link protocol must be configurable to switch between PPP in HDLC and LAPD framing.

e. CLNP and IP Encapsulation

This specification defines the encapsulation of one network layer protocol within another. The CLNP packets shall be encapsulated over IP using Generic Routing Encapsulation (GRE) as payload in an IP packet with an IP protocol number and Don't Fragment (DF) flag not set. It shall contains an Ethertype to indicate what network layer protocol is being encapsulated. The IP packets shall be encapsulated over CLNS using Generic Routing Encapsulation (GRE) as payload of a CLNP Data Type PDU with an NSAP selector value and segmentation permitted (SP) flag set.

f. CLNP and IP Tunneling

The standard specifies the Network Layer PDU Tunneling Function to provides a static tunnel between two Data Communications Function (DCF)s supporting the same network layer PDU. Any IP packet that cannot be forwarded due to its size larger than the MTU, with DF bit set should be discarded and generate an ICMP unreachable error message.

g. CLNP and IP Forwarding

The standard defines the Network Layer PDU Forwarding Function to forwards the CLNP and/or IP network layer packets according to their respective recommendations.

h. CLNP and IP Routing

The standard specifies the Network Layer PDU Routing Function, as its name implied, to route network layer packets. A DCF supporting OSI routing shall support IS-IS while a DCF supporting IP routing shall support Integrated IS-IS and may also support OSPF and other routing protocols.

i. CLNP and IP Interworking

The standard specifies the Network Layer PDU Interworking Function to ensure neighboring DCF functions running different network layer protocols (CLNP and/or IP) can communicate.

2. New Updates

The New ITU-T recommendation G.7712/Y.1703 'Architecture and Specification of Data Communication Network', was approved on March 12, 2003 by ITU SG15 [11]. Equipment vendors such as Lucent, Nortel and Marconi collaborated to define the G.7712 standard. The standard is also a key building block for GMPLS, a protocol that ensures optimal routing and best network resource usage in combined IP, optical and circuit switching networks. The latest revision adds the support of connection-oriented network for new services such as ASTN in addition to the original data communications functions that support connection-less network services for TMN provided in the 11/2001 version. It allows the use of IP protocols as well as OSI protocols, through communication among the transport plane, the control plane, and the management plane. It also promotes automatic encapsulation to allow the IP traffic to cross over legacy OSI DCN as well as allows OSI traffic to cross new IP DCN.

The details of the new features are summarized in the following sections:

a. Terms and definitions

It added in new terms and definitions for IP routing InterWorking Function, Network-Layer InterWorking Function and Automatically Encapsulating Data Communications Function (AE-DCF).

b. Reliability of Signaling Communications Network (SCN)

It inserted a line to mentioning that one way of achieving a reliable SCN is through use of Packet 1+1 protection for connection-oriented protocols such as MPLS.

c. SCN Data Communication Functions

It mentioned that the DCF within the ASTN entities may operate as an Label Edge Router (LER), Label Switch Router (LSR) and support the following functions:

(1) MPLS PDU into ECC Data-Link Layer Encapsulation Function
(2) MPLS PDU into Ethernet Frame Encapsulation Function
(3) MPLS LSP Signaling Function
(4) MPLS LSP Forwarding Function
(5) MPLS LSP path Computation Function
(6) Network Layer Packet into MPLS Encapsulation Function

It also stated the minimum requirements to provide packet 1+1 protection services for the network as well as both Ingress and Egress nodes.

d. Network Layer PDU into SDH ECC Data-Link Frame Encapsulation Function

For IP-only interface, it required both transmit and receive ends to have IS-IS packets identified in the PPP Information and Protocol Fields. For OSI-only interface, it needed the transmit end to put CLNP, ISIS and ESIS packets directly into LAPD. For both IP + OSI interface, it wanted the dual interface that supports PPP as data-link protocol to have the CLNP, ISIS and ESIS packets directly into PPP Information Field and the OSI protocol value into the PPP Protocol Field at the transmit end. For the dual interface that support LAPD as data-link protocol, the CLNP, ISIS and ESIS packets should be put directly into LAPD payload at the transmit end.

e. Network Layer PDU Encapsulation Function

As an option, the Network Layer PDU Encapsulation function may forward PDUs across incompatible nodes via the automatic encapsulation procedure described in Annex B as spelt out in the standard. Take note that the DCF supporting the automatic encapsulation procedure is compatible with and can be deployed in the same area as a DCF that does not support the automatic encapsulation procedure.

f. Integrated ISIS Requirements

New paragraphs describing the Network-layer Protocol Aware Adjacency Creation are added. In summary, it described what are the protocols supported by the DCF and the tasks the DCF should perform with and with no adjacency exists with the neighbor.

g. MPLS PDU into ECC Data-Link Layer Encapsulation Function

This is a new section added in to explain the function of encapsulate and unencapsulate a MPLS PDU into an ECC Data-Link Layer frame. At the Transmit end, it shall put MPLS packets directly into PPP Information Field with MPLS protocol value of 0281 hex into the PPP Protocol Field for MPLS Unicast. At the receive end, it shall identify an MPLS packets if the PPP Protocol Field has the with MPLS protocol value of 0281 hex for MPLS Unicast.

h. MPLS PDU into Ethernet Frame Encapsulation Function

This is a new section added in to explain the function of encapsulate and unencapsulate a MPLS PDU into an Ethernet frame. It shall encapsulate MPLS PDUs into Ethernet frames using an Ethertype value of 8847 hex for MPLS Unicast.

i. MPLS LSP Signaling Function

This is a new section added in to explain the MPLS LSP Signaling function to provide the necessary signaling to set-up the MPLS LSP. The DCF shall support the Explicit Path with a strict route via simple nodes for point-to-point unicast LSP reservation model.

j. MPLS LSP Forwarding Function

This is a new section added in to explain the MPLS LSP Forwarding function that forwards the incoming MPLS packets to an outgoing interface based on its MPLS label and the Next Hop Label Forwarding Entry (NHLFE). The sequence of packets must be maintained within an LSP.

k. MPLS LSP Path Computation Function

This is a new section added in to explain the MPLS LSP path Computation function that calculates the path for a unidirectional LSP. It shall also calculate the paths for two unidirectional LSPs to the same destination such that their paths do not traverse the same node or subnetwork.

l. Network Layer Packet into MPLS Encapsulation Function

This is a new section added in to explain the function that adds or removes the MPLS label stack entry to or from the network layer packet as described in RFC 3032.

m. MPLS Packet 1+1 Protection Function

This is a new section added in to explain the MPLS Packet 1+1 Protection functions. The ingress and egress nodes shall identify and associate the two LSPs providing packet 1+1 protection service via either network management interface or signaling. The sequence number shall be used as the identifier for packet 1+1 protection. Each copy of the dual-fed packet is assigned the same unique sequence number by the ingress node. The sequence number of the next packet is generated by adding one to the current sequence number.

n. Requirements for Three-way Handshaking

This section is modified to explain the requirements for the Three-way Handshaking function for the DCF that supports the Integrated IS-IS protocol for each point-to-point circuit that has an adjacency three-way state.

o. Requirements for Automatic Encapsulation

This is a new Annex added in to provide the specification for the optional AE-DCF that enables nodes that support routing of differing incompatible network layer protocols, such as CLNS, IPv4 or IPv6 to be present in a single IS-IS level 1 area or level 2 subdomain. It shall automatically encapsulates one network layer protocol into another as required, assuming all the nodes support IS-IS or Integrated IS-IS routing.

p. Example Implementation of Automatic Encapsulation

This is a new Appendix added in to provide some brief example details on how a node may be implemented with respect to one aspect of the feature specified in the standard.

q. Commissioning Guide for SDH NEs in Dual RFC 1195 Environment and Impact of Automatic Encapsulation Option

This is a new Appendix added in to provide guidance on installing the Integrated IS-IS nodes in a dual IPv4 and OSI network. It also explained how to use the optional automatic encapsulation feature described in Annex B of the standard.

r. Example Illustration of Packet 1+1 Protection

This is a new Appendix added in to provide an example to illustrate how the Packet 1+1 protection function can be realized and implemented.

G. SUMMARY

This chapter examined the definitions and usage of DCC, DCN, OSI and SNMP (IP) used by the network management of SONET/SDH. The need for IP over the DCC was reviewed. It was followed by the first objective of the thesis study: examine the main features and new updates available in the ITU-T G.7712 standard.

In the next chapter, we will look at the response and support from the telecommunication industry about this standard before performing some traffic analysis on the two different routing protocols, IS-IS and OSPF defined in the G.7712 standard by using Opnet.

THIS PAGE INTENTIONALLY LEFT BLANK

V. PERFORMANCE ANALYSIS

A. CHAPTER OVERVIEW

In this chapter, we will look at the response and support from the telecommunications industry for the ITU-T G.7712 standard. We then perform some traffic analysis by creating an Opnet model to simulate the packet flow within a SONET DCC network and determine the differences and characteristics of the two routing protocols, IS-IS and OSPF defined in the G.7712 standard.

B. INDUSTRY SUPPORT

A survey was done to determine the support of the ITU-T G.7712 standard by some of the major SONET/SDH vendors in the telecommunications industry. Five vendors were selected: Alcatel, Cisco, ECI, Marconi and Nortel. [12,13]

1. Alcatel 16xx Optical Families

Alcatel manufactures the 1356DCN NMS that supports the G.7712 standards to manage their 16xx Optical products. It can manage both OSI and IP networks dedicated to the DCN of transmission networks [14].

2. Cisco ONS 15600

The Cisco ONS 15600 Multiservice Switching Platform supports the G.7712 standards and is managed by its NMS, the Cisco Transport manager. Similar to Alcatel, it can manage both OSI and IP networks dedicated to the DCN. [15]

3. ECI Syncom & XDM

ECI's NMS, eNM does not support the G.7712 standards to manage their Syncom & XDM Optical families. Instead, they support the MTMN v2 standards to make umbrella management under a TMN environment simpler to implement [16].

4. Marconi MSH2K

Marconi's NMS currently supports only the OSI stack management and the embedded DCN's are OSI-based (i.e. the DCC carries OSI stack protocols and not IP packets). The NMS manages the NE with a Q/OSI interface. Marconi

plans to have automatic encapsulation support for IP + OSI DCN's in their latest products. [17]

5. Nortel OPTera Metro 3000

Nortel OPTera Metro 3000 supports the G.7712 standards for both IP and OSI management. It requires a Network Processor (NP) in order to support TCP/IP for management. The NP acts as a gateway to the OSI stack of all Shelf Processors (SPs) within the NP's Span of Control. The SP can be connected directly to using either X.25 or OSI interface [13].

It can be seen that out of the five vendors selected, all four vendors except ECI support or plan to support OSI and IP networks dedicated to the DCN. ECI in general only marginally support OSI DCN networks.

C. TRAFFIC ANALYSIS

OPNET IT Guru 10.0 is a modeling and simulation tool that provides an environment for analysis of communication networks. However, it does not have a SONET DCC model in its standard model library. Thus a SONET DCC network model was created to facilitate our simulation of IS-IS and OSPF routing protocols as defined in the G.7712 standard. Three different scenarios were created using this OPNET model to simulate the packet flow within the SONET DCC network to understand the differences and characteristics of the two routing protocols.

1. Simulation Assumptions and Parameters

In order to simulate such a SONET DCN in an OPNET model, many assumptions and simplifications were necessarily made:

a. No attempt was made to model the actual geometry or layout of the SONET DCN.

b. There is one server and four workstations. The servers run two main applications, database access and telnet sessions to mimic the types of transactions that the users will need to access. The configurations and settings for these application simulations are shown in Figures 19 - 21.

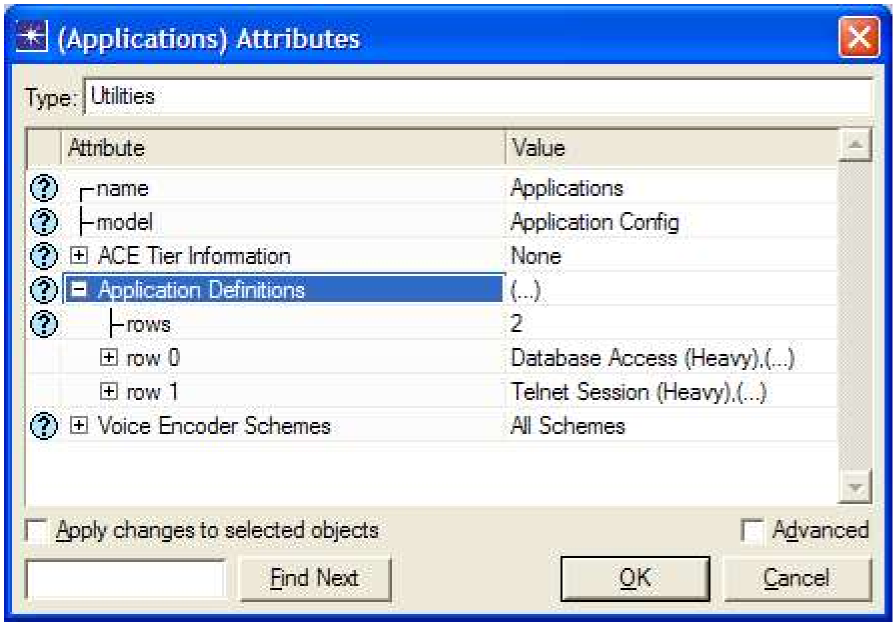

Figure 19. Applications Configuration

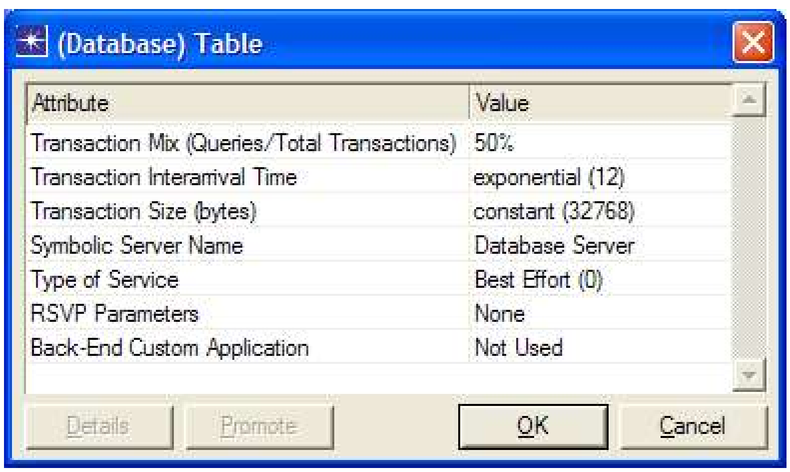

Figure 20. Database Access Table

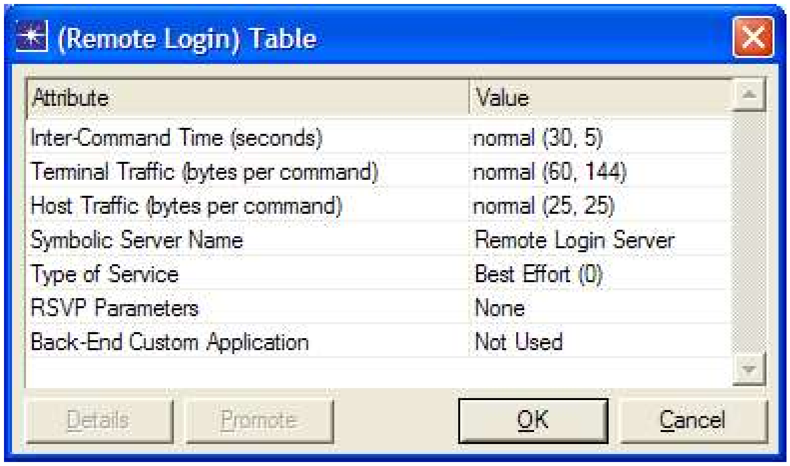

Figure 21. Telnet Session Table

c. The routers in the simulation are not really pure routers, they are used in this simulation to represent the routing functions in the SONET equipment which are running either the IS-IS or OSPF protocol in the DCC environment.

d. Two different user profiles were assumed: System Administrator and Remote User. These two profiles attempt to mimic the types of users that would be using SONET DCN. The definitions of the profiles are shown below in Figure 22:

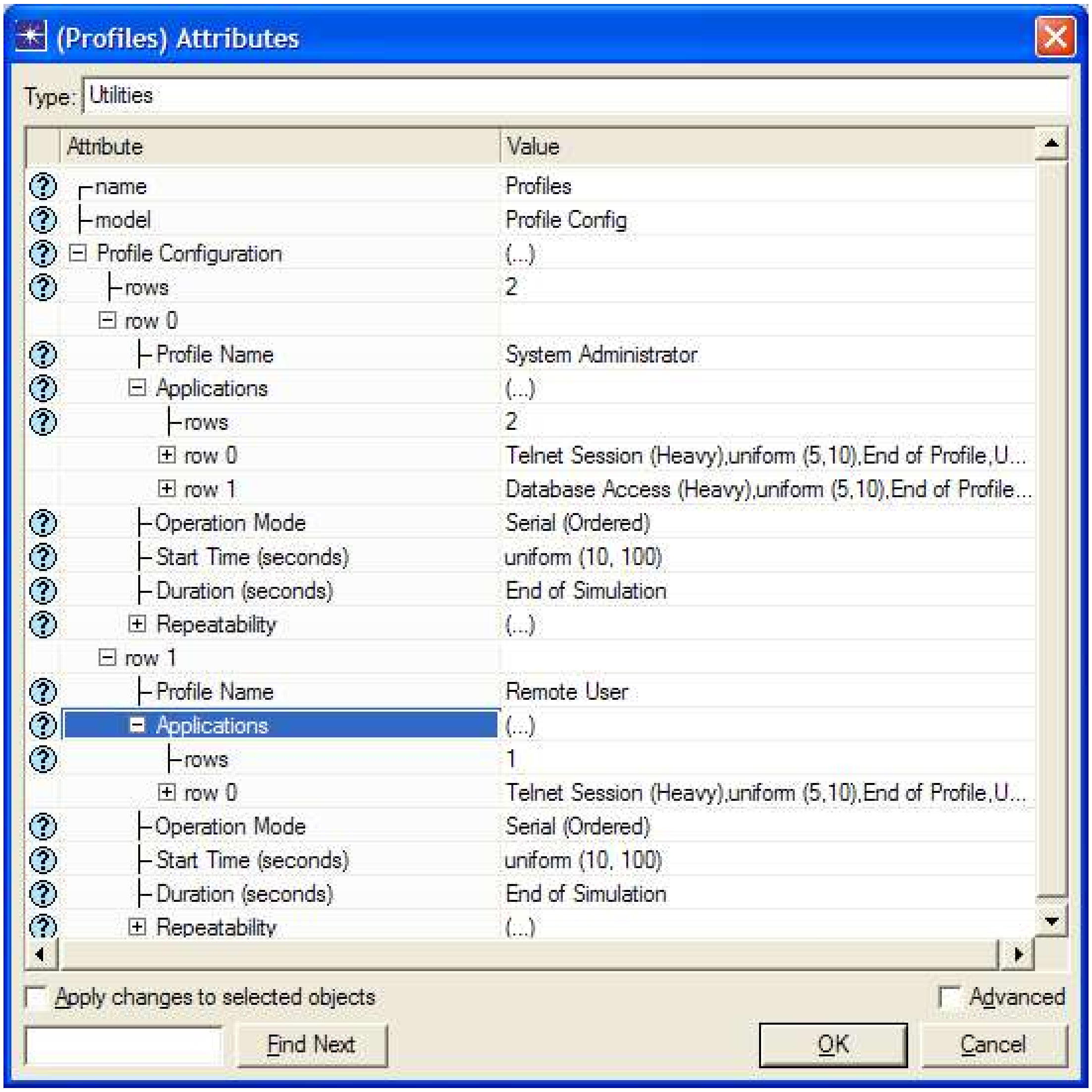

Figure 22. Profiles Configuration

The network configuration for this study consists of a server, workstations and routers and is depicted in Figure 23 below.

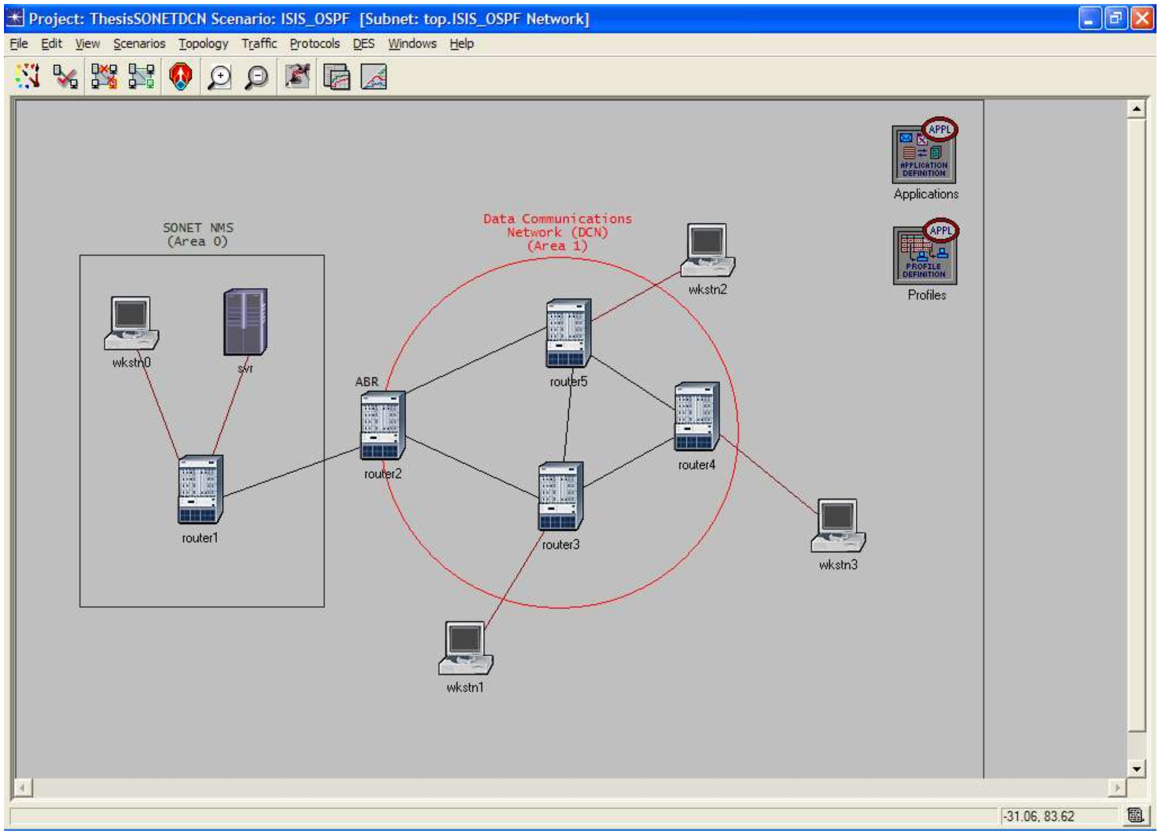

Figure 23. SONET DCC Network in OPNET

Workstation 0 (wkstn0 in Figure 23) and the server are located on the same premises as the SONET equipment whereas the other workstations are located at other sites. These workstations are indirectly connected to the server via their local routers which are configured to form the DCN for network management of the optical network. The data rate of the links connecting these workstations to the routers is 768 kbps (simulating the data rate of DCC in the SONET frame).

For every simulation, applications are assumed to have a uniformly distributed start time offset with a minimum of ten seconds and maximum of 100 seconds. They are assumed to have unlimited repeatability. The user profiles are assumed to randomly access applications in a serial fashion (i.e., one at a time). The profile "log-on" times are uniformly distributed, with a minimum of one second and maximum of 500 seconds. Profile repeatability is also unlimited.

2. Test Scenarios

In order to check the characteristics of the IS-IS and OSPF routing protocols, three test scenarios were created by varying the routing protocols. The first simulation of the OSPF protocol was run in OPNET using the above parameters. The second simulation was run with the same parameters as the first, except that the protocol used was assumed to be IS-IS for both routers 1 & 2 while the rest of the routers were still using OSPF. The final simulation was run in OPNET using IS-IS protocol for all routers. All test scenarios were performed using the network configuration as shown in Figure 23. The objective of each experiment scenario was to evaluate performance metrics, such as Ethernet delay, server performance, link throughput, link utilization and link usage that are available in OPNET, collected after the simulation.

These performance metrics were studied because Ethernet delay serves to identify the time taken for a packet to travel across multiple links to the destination. Assuming consistent behavior by the routing protocols, this is considered a reasonable measure of the impact on services that router functions – such as router specific messages or the choice of path length – will have on network performance. Server performance measures the time taken for the server to process a request from the workstations. Since the remote workstations are dispersed throughout the network, both Ethernet delay and server performance provide a good indication of potential bottlenecks and areas of congestion. A low value of either Ethernet delay or server performance indicates a network that is functioning efficiently with minimal overhead intrusion from the routing protocol.

Similarly, link throughput provides a good measure for projected demand and potential performance-related problems. It is important to understand that link throughput is a time-averaged value. Since link throughput is the ratio of data sent to the time spent sending it, better routing performance can be inferred by lower values of link throughput. This is because an efficient routing protocol will send fewer overhead messages.

On the other hand, utilization indicates the percentage of loading on the link capacity over a specified period of time. Link utilization is defined as the ratio of link throughput over link data rate and it is closely related to network congestion and response time. Again, a lower value of link utilization indicates the network is not congested with routing overhead. Link utilization is used in this simulation to represent the traffic loading based on profiles of the users accessing the server via the workstations.

3. Discussion of Simulation Results

The test scenarios vary the type of routing protocols to determine the optimum performance within the network. Figure 24 to 31 illustrate comparisons between results of these protocols. The performance metrics studied were the Ethernet delay, server performance, link throughput, link utilization and link usage.

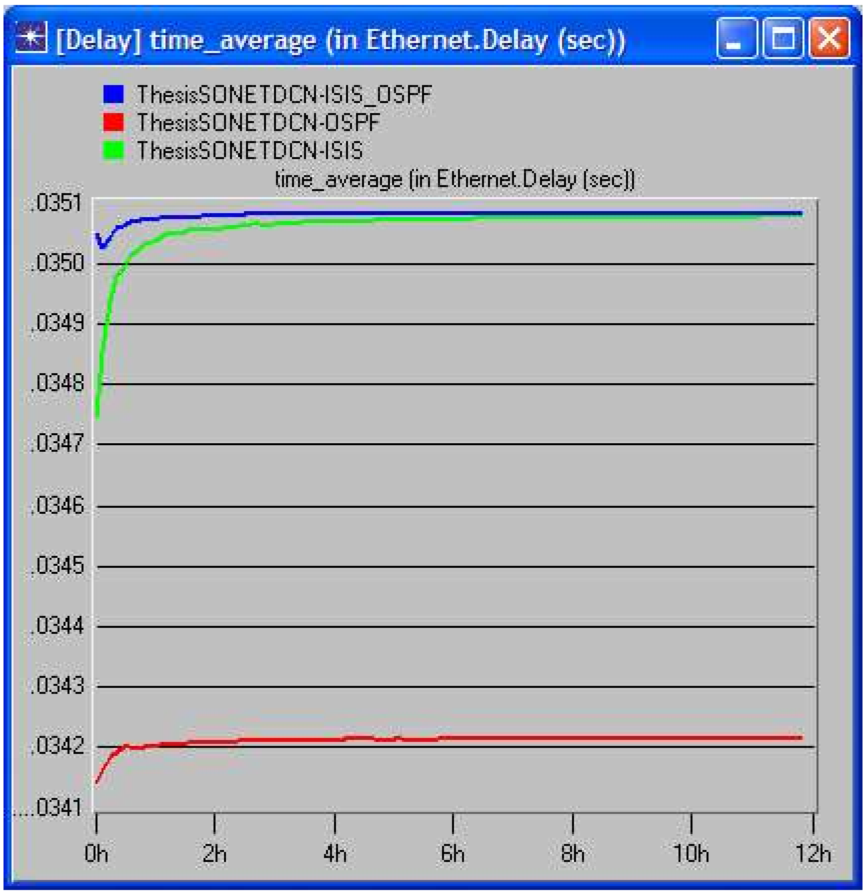

Figure 24. Ethernet Delay

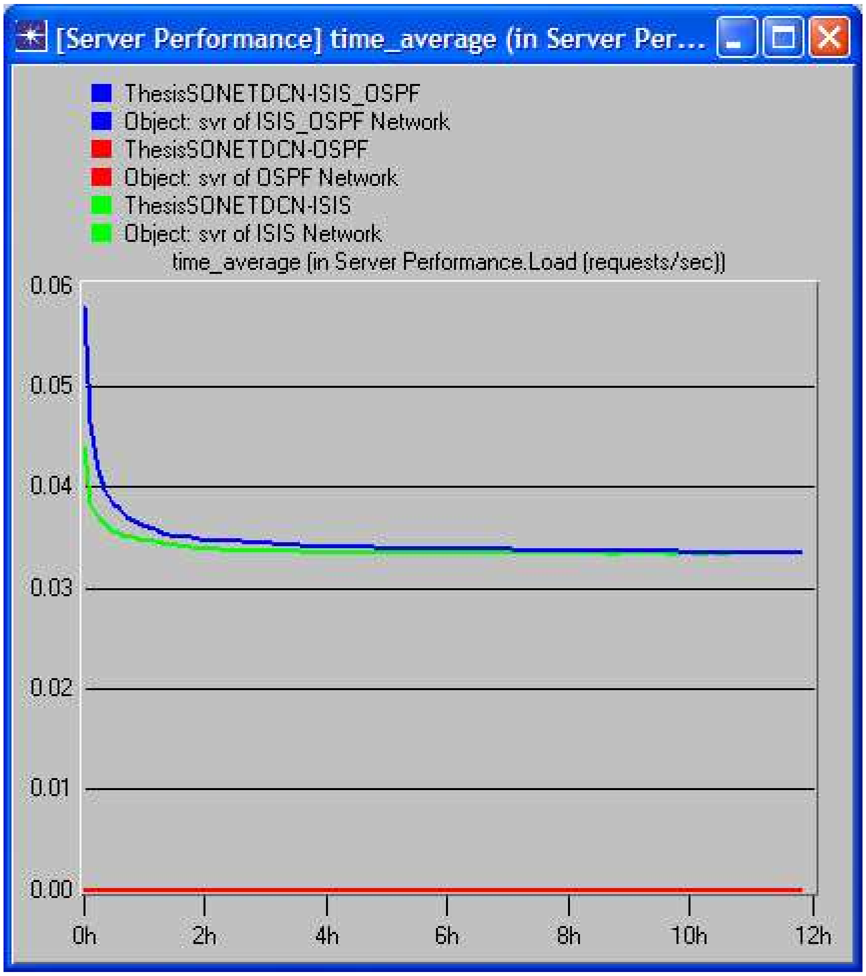

Figure 25. Server Performance

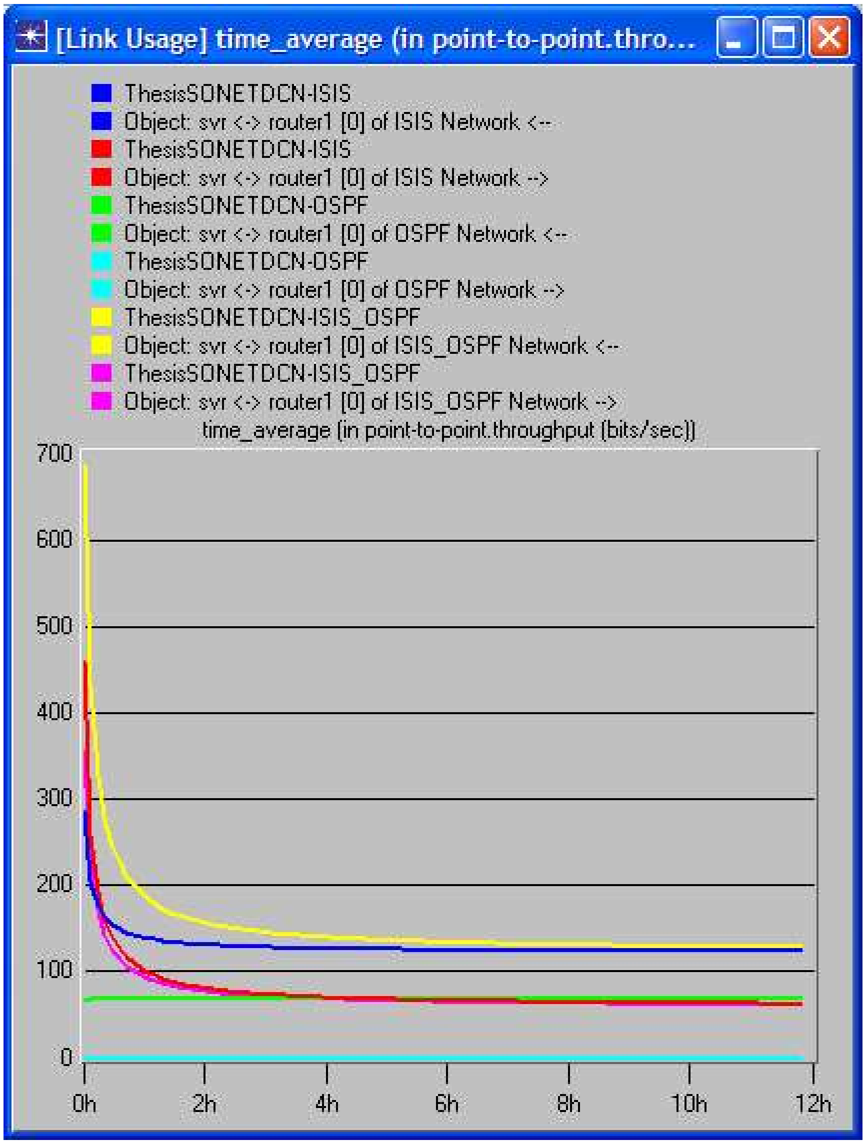

Figure 26. Link Throughput between Server and Router 1

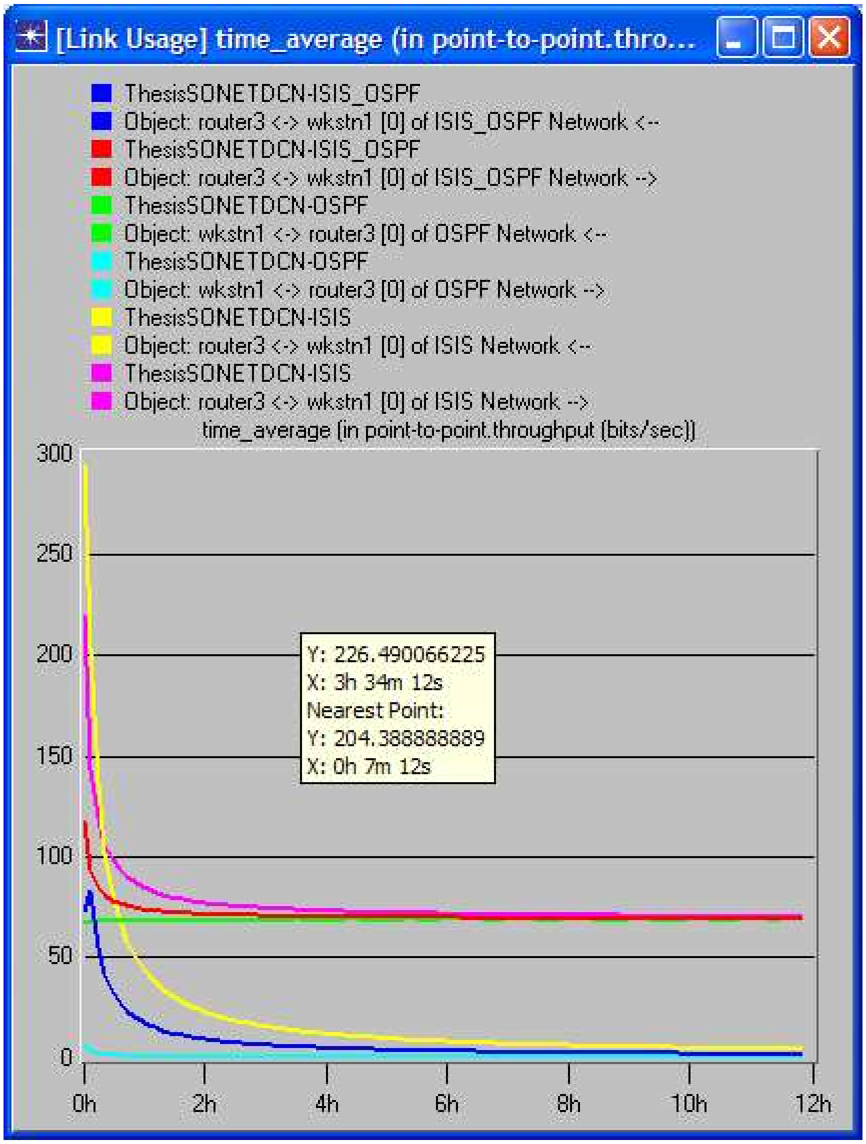

Figure 27. Link Throughput between Workstation 1 and Router 3

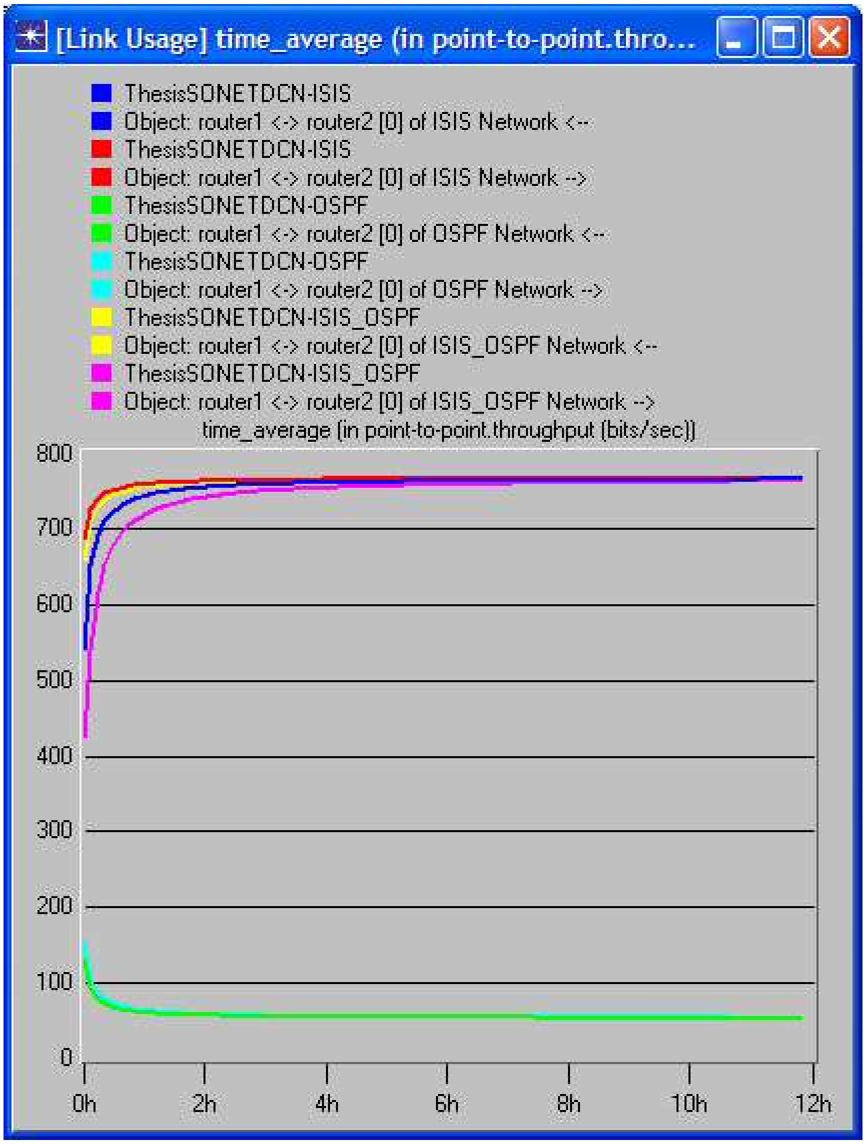

Figure 28. Link Throughput between Router 1 and Router 2

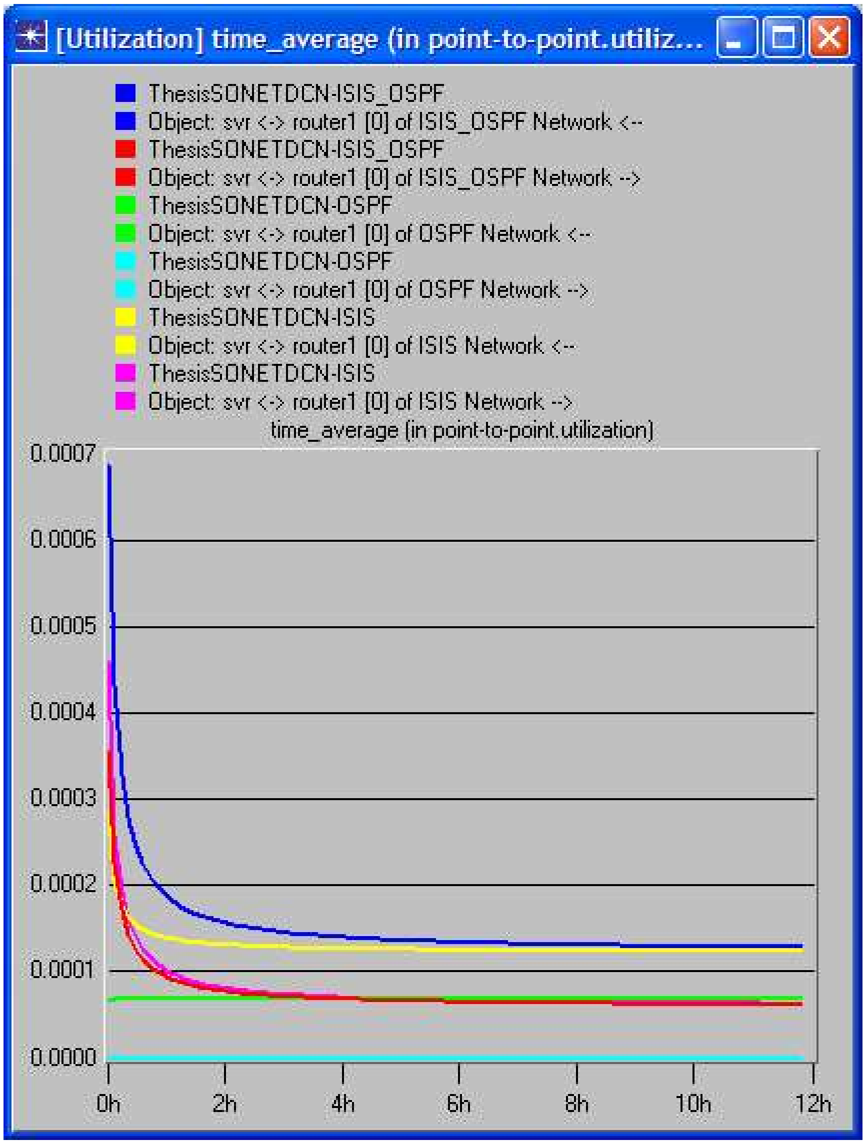

Figure 29. Link Utilization between Server and Router 1

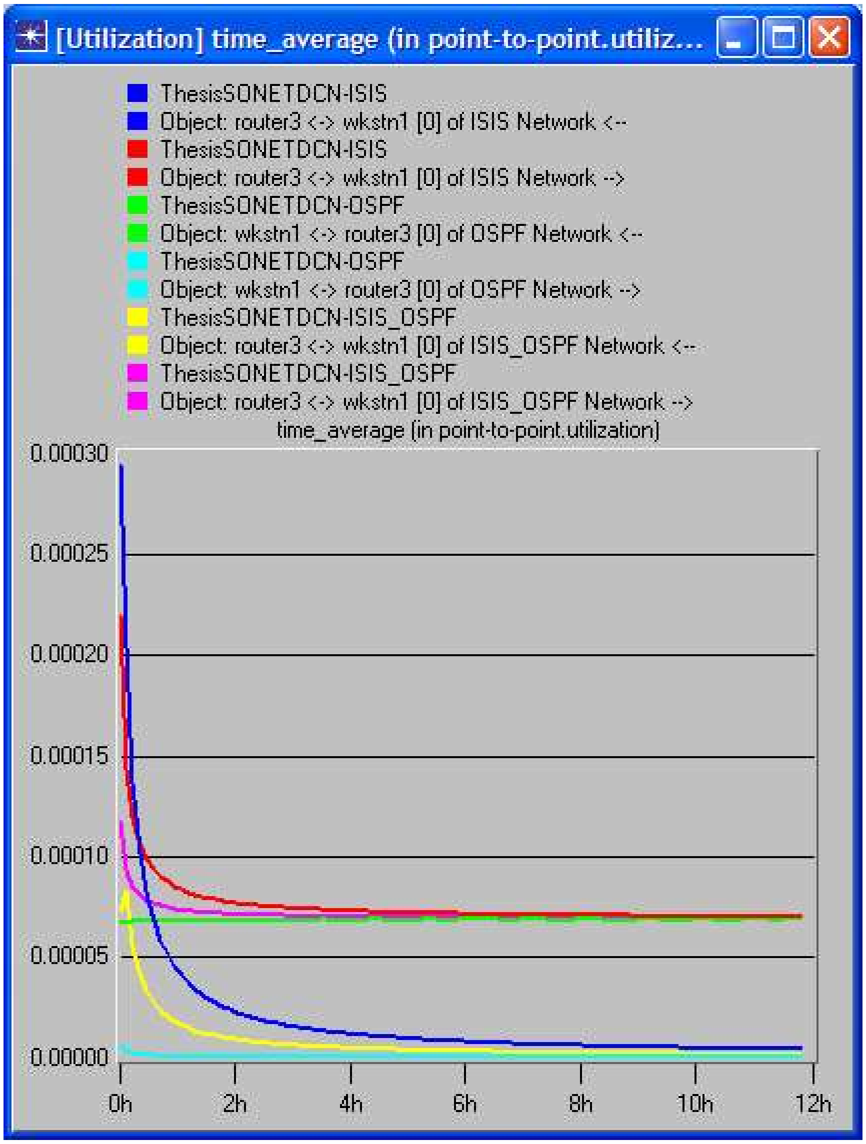

Figure 30. Link Utilization between Workstation 1 and Router 3

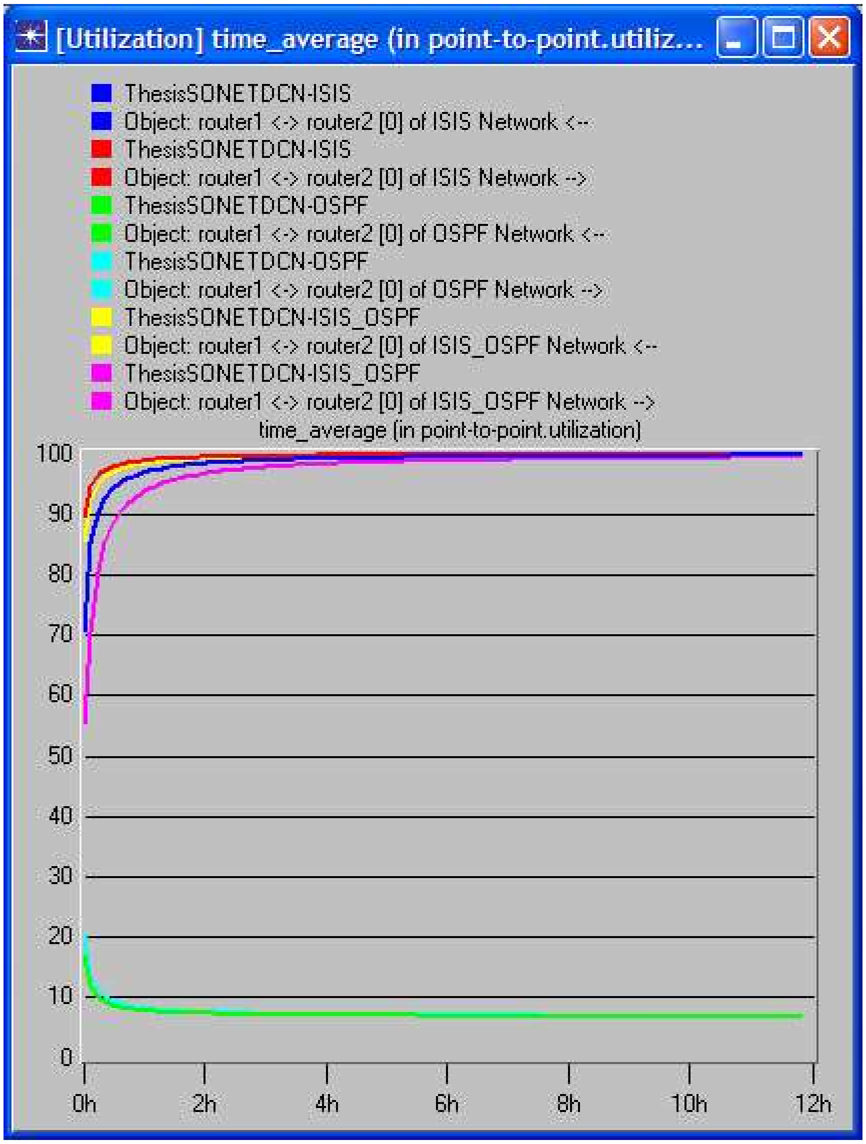

Figure 31. Link Utilization between Router 1 and Router 2

a. *Results of OSPF Routing Protocol*

This experiment was designed to explore the effects of OSPF routing protocol within the SONET DCN network. The assumption made in this experiment is that the OSPF protocol facilitates all the connections between workstations and the server via the routers as well as all the connections between routers.

Figure 24 shows the result of Ethernet Delay. The time average of the Ethernet delay in the OSPF DCN network is around 0.0342 seconds and is

the lowest when compared to the other two scenarios. It shows that it is more efficient to route the data via a pure OSPF protocol. By design, OSPF uses very few overhead messages to update network nodes. Figure 25 shows the result of server performance. The average time taken for the server to respond back to the workstations requests is negligible. This is also the lowest amongst the three scenarios.

Figures 26 to 28 show the result of link throughput. Since the result for a single measurement of end-to-end throughput from server to workstation cannot be generated by OPNET, three separate measurements are evaluated and can be used to represent the end-to-end throughput when combined. Figure 26 shows the link throughput between the server and router 1. The time average of the link throughput is about 70 bits per second from router to server while nearly zero bits per second from server to router. The second graph shows the plot of link throughput between workstation 1 and router 3. The time average of the link throughput is about 70 bits per second from router to workstation while nearly zero bits per second from workstation to router. The third graph shows the plot of link throughput between router 1 and router 2. The time average of the link throughput is about 60 bits per second between router 1 & 2. The link throughput is the lowest amongst the three scenarios. The end-to-end throughput derived from combining the results of these three figures will indicate that a pure OSPF routing protocol will take the shortest time to route the requests from workstation to the server.

Figure 29 to 31 shows the result of link utilization. The first graph shows the plot of link utilization between server and router 1. The time average of the link utilization is about 0.00008% from router to server while nearly zero 0% from server to router. The second graph shows the plot of link utilization between workstation 1 and router 3. The time average of the link utilization is about 0.00007% from router to workstation while nearly 0% from workstation to router. The third graph shows the plot of link utilization between router 1 and router 2. The time average of the link utilization is about 8% between router 1 & 2. The link utilization is the lowest amongst the three scenarios. Likewise, the end-to-end

utilization derived from combining the results of these three figures is the lowest for a pure OSPF protocol to route the traffic across the DCN.

b. Results of IS-IS and OSPF Protocols

This experiment was designed to explore the effects of IS-IS and OSPF routing protocols within the SONET DCN network. The assumption made in this experiment is that IS-IS protocol is applied to the connection between routers 1 & 2 while the rest of the routers are still using OSPF.

Figure 24 shows the result of Ethernet delay. The time average of the Ethernet delay in the OSPF DCN network is around 0.03507 second and is the highest when compare to the other two scenarios. Figure 25 shows the result of server performance. The time average of the server performance load is about 0.034 requests per second. This is also the highest amongst the three scenarios.

Figure 26 to 28 shows the result of link throughput. The first graph shows the plot of link throughput between server and router 1. The time average of the link throughput is about 135 bits per second from router to server while nearly 70 bits per second from server to router. The second graph shows the plot of link throughput between workstation 1 and router 3. The time average of the link throughput is about 70 bits per second from router to workstation while nearly 7 bits per second from workstation to router. The third graph shows the plot of link throughput between router 1 and router 2. The time average of the link throughput is about 750 bits per second between router 1 & 2.

Figure 29 to 31 shows the result of link utilization. The first graph shows the plot of link utilization between server and router 1. The time average of the link utilization is about 0.000135% from router to server while about 0.00007% from server to router. The second graph shows the plot of link utilization between workstation 1 and router 3. The time average of the link utilization is about 0.00007% from router to workstation while about 0.000005% from workstation to router. The third graph shows the plot of link utilization between router 1 and router 2. The time average of the link utilization is about 98.9% between router 1 & 2.

c. *Results of IS-IS Routing Protocol*

This experiment was designed to explore the effects of IS-IS routing protocol within the SONET DCN network. The assumption made in this experiment is that IS-IS protocol facilitates all the connections between workstations and server via the routers as well as all the connections between routers.

Figure 24 shows the result of Ethernet delay. The time average of the Ethernet delay in the OSPF DCN network is around 0.03506 second and is in the middle when compare to the other two scenarios. Figure 25 shows the result of server performance. The time average of the server performance load is about 0.033 requests per second. This is also in the middle amongst the three scenarios.

Figure 26 to 28 shows the result of link throughput. The first graph shows the plot of link throughput between server and router 1. The time average of the link throughput is about 125 bits per second from router to server while nearly 70 bits per second from server to router. The second graph shows the plot of link throughput between workstation 1 and router 3. The time average of the link throughput is about 75 bits per second from router to workstation while nearly 10 bits per second from workstation to router. The third graph shows the plot of link throughput between router 1 and router 2. The time average of the link throughput is about 750 bits per second between router 1 & 2.

Figure 29 to 31 shows the result of link utilization. The first graph shows the plot of link utilization between server and router 1. The time average of the link utilization is about 0.000125% from router to server while about 0.00007% from server to router. The second graph shows the plot of link utilization between workstation 1 and router 3. The time average of the link utilization is about 0.00007% from router to workstation while about 0.00001% from workstation to router. The third graph shows the plot of link utilization

between router 1 and router 2. The time average of the link utilization is about 98.9% between router 1 & 2.

d. Comparison of the Effects of Different Routing Protocols

With all the results obtained from Figure 24 to 31, we can now analyze the effects of the different routing protocols presented in the three different scenarios.

From the results obtained from Figure 24, the OSPF DCN network experiences the lowest Ethernet delay in the network. The other two scenarios running IS-IS routing protocols have higher Ethernet delay. Further, the pure IS-IS DCN network takes a longer time to reach the steady state when more traffic is generated in the DCN network. It shows that a pure OSPF protocol is the most efficient routing protocol to route data over the DCN.

As shown in Figure 25, the results show that a pure OSPF DCN network has the lowest average time taken for the server to respond back to the workstations requests. For comparison, the other two scenarios have almost identical results when the server processes the workstation's requests. This shows that the server is most efficient in processing the data when the workstation requests are routed via OSPF protocol in the DCN as compared to either a pure IS-IS or mixed IS-IS with OSPF protocols when applied to the DCN.

Figure 26 to 28 presented the results of link throughput. In general, the DCN network running pure OSPF routing protocol has the lowest link throughput with the traffic flow between the server and workstations. The link throughput is almost similar for the other two scenarios running IS-IS routing protocols but there are slight differences. The hybrid IS-IS and OSPF DCN network has a slightly higher link throughput between server and router 1 as compared to the pure IS-IS DCN network as protocol translation from OSPF to IS-IS is needed from all traffic generated from the other workstations when routed to their respective routers before entering router 1.

The results of the link utilization are shown in Figure 29 to 31. Similar to the results of the link throughput, the DCN network running pure OSPF routing protocol has the lowest link utilization, be it traffic flowing from the routers to the server and workstations or traffic generated from the server and workstations to the routers. This is due to the fact that there is no routing protocol translation needed in the network. For the other two scenarios running IS-IS routing protocols, the link utilization is almost similar but there are slight differences. The hybrid IS-IS and OSPF DCN network is has slightly higher link utilization between server and router 1 as compared to the pure IS-IS DCN network. Similar to the arguments given for the link throughput, this is because protocol translation from OSPF to IS-IS is needed from all traffic generated from the other workstations when routed to their respective routers before entering router 1.

The overall results show that a pure OSPF protocol for DCC network is the way forward as its performance is the best. ISIS-OSPF is just a interim for the DCC network to perform in the same way as a pure ISIS (OSI) DCC network solely used in the SONET/SDH world. Thus G.7712 in specifying the IP network for the DCC network is the way to go and thus, most SONET/SDH vendors are moving in that direction as highlighted in the earlier paragraphs.

D. SUMMARY

This chapter presented an overview of the responses and supports gathered from the Telecommunication industry to the G.7712 standard. Subsequently, the modeling of both OSPF and IS-IS routing protocols within a SONET DCN Network was created using OPNET. It outlined three test scenarios used for the simulation and presented the simulation results and the effects on each routing protocols.

The next chapter summarizes the findings from this study and presents possible areas for future work.

VI. CONCLUSION

A. CHAPTER OVERVIEW

This chapter provides a summary of the findings of this study. Included in the summary are conclusions from observations made during the execution of this study. Suggestions for future and follow-on work are also presented.

B. OUTCOME OF RESEARCH

This thesis project has provided the author with many learning opportunities regarding the G.7712 ITU-T standard and its usefulness and presence in the telecommunication industry.

The first part of this study involved study into the main features and new updates available in the ITU-T G.7712 standard. The push for an eventual IP DCN for managing the SONET network is obvious. The key element in the standard is offering the integrated IS-IS protocol for routing IP and CLNP traffic across the DCN. This protocol allows the use of IP protocols as well as OSI protocols, through communication among the transport, control and management plane of the network. It also promotes automatic encapsulation to allow the IP traffic to cross over a legacy OSI DCN as well as allow OSI traffic to cross the new IP DCN.

Subsequently, a SONET DCN model was created using OPNET to allow various test scenarios to be simulated for exploring the effects of both OSPF and IS-IS routing protocols. From the results obtained, we found that a pure OSPF DCN network is the best amongst the three different scenarios. It has the lowest Ethernet delay and the best server-workstation performance in the network. It also has the lowest link throughput and link utilization in the network.

On the other hand, both the scenarios running pure IS-IS and hybrid IS-IS and OSPF routing protocols have higher delays and longer processing time in the network. They also experience higher link throughput and utilization in the network. The simulation results obtained for these two scenarios are almost

identical but there are some slight differences. The Ethernet delay, server performance, link throughput and link utilization are typically higher for a hybrid IS-IS and OSPF DCN network when traffic transverses through router 1 and require communications with the server. This is because protocol translation from OSPF to IS-IS is needed from all traffic generated from the other workstations when routed to their respective routers before entering router 1 and the server. However, a pure IS-IS DCN network takes a longer time to reach the steady state for the Ethernet delay when more traffic is generated in the DCN network.

The difference between a pure IS-IS and hybrid IS-IS and OSPF DCN network is not really significant when compared to a pure OSPF DCN network. Deploying hybrid IS-IS and OSPF routing protocols should be seen as the direction for the SONET DCN implementation when more and more SONET equipment vendors are deploying G.7712 standard with their equipment. Eventually a pure OSPF DCN is recommended when all the SONET vendors began to realize the benefits and usefulness of OSPF routing in an IP based DCN network.

C. FUTURE RESEARCH AREAS

The results of this research can be construed as accurate in so far as one acknowledges the myriad assumptions and simplifications. Further research should be conducted with more realistic representations of the target network by modeling the SONET network using the models found in the OPNET WDM Guru.

In addition, a test network can be setup in the laboratory once the actual SONET hardware and software have arrived and the network analysis tool can be installed into the SONET network management system to analyze the results. The test scenarios generated in this study could be reproduced and actual traffic data obtained from the SONET DCN testbed can be used to compare with the OPNET analysis performed in this study.

LIST OF REFERENCES

1. “SONET Architecture 101: A Tutorial for Datacommers,” Features, TCPMag.com for Cisco Internetworking Experts, *http://tcpmag.com/features/article.asp?EditorialsID=53*, last accessed 21 August 2003.

2. “ITU-T Recommendations G.7712/Y.1703 (11/2001) – Architecture and Specifications of data communication network,” International Telecommunication Union, dated 29 November 2001.

3. “SONET/SDH Description,” Technical Information, Interface Bus, *http://www.interfacebus.com/Design_Connector_SONET.html*, last accessed 14 August 2003.

4. “SONET Graphical Overview,” Technical Report, Cisco Technote, *http://www.cisco.com/en/US/tech/tk482/tk607/technologies_tech_note09186a0080124afa.shtml*, last accessed 14 August 2003.

5. “SONET,” Technical Paper originated from D.K. Siu of Worcester Polytechnic Institute (c. ~1997), *http://www.techfest.com/networking/wan/dks1/dks1.htm*, last accessed 21 August 2003.

6. “Standards & Protocols: SONET Frame Structures,” Online Resources for comms design engineers, Features, Comms Design, *http://www.commsdesign.com/main/1999/03/9903standards.htm*, last accessed 21 August 2003.

7. “DCC Solutions for SONET/SDH Systems,” Technical Report, OpenCon systems, Inc., Version 1.0, October 2003, *http://www.opencon.com/dcc/DCC-white-paper-Rev2.pdf*, last accessed 21 August 2003.

8. “References on Optical Network and IP over DWDM,” Reference, *http://www.cs.wustl.edu/~jain/refs/opt_refs.htm*, last accessed 21 August 2003.

9. “Need for an IP Standard on the SONET Section DCC, Draft Document dated 13 September 2000, Network and Services Integrated Forum (NSIF), *http://www.atis.org/pub/sif/se/se009038.doc*, last accessed 21 August 2003.

10. “FAA Handbook,” Technical Document, FAA, *http://204.108.5.10/nasiHTML/FAAStandards/faa-hdbk-002/text.html*, last accessed 21 August 2003.

11. “ITU-T Recommendations G.7712/Y.1703 (03/2003) – Architecture and Specifications of data communication network,” International Telecommunication Union, dated 12 March 2003.

12. “IP Management Gains Favor,” Light Reading, http://www.lightreading.com/document.asp?doc_id=43912, last accessed 23 September 2006.

13. “Vertel Supports G.7712, Latest Optical Network Management Standard,” Embedded Stars, http://www.embeddedstar.com/press/content/2003/3/embedded7896.html, last accessed 23 September 2006.

14. “Alcatel 1354RM Rel.6.3 Operator’s Handbook,” 1st Edition, Alcatel, 2006.

15. “Optical Release 6.0: Scalable and Flexible Carrier-Class Solutions,” Cisco, http://www.cisco.com/en/US/products/hw/optical/products_announcement0900aecd80319724.html, last accessed August 2006.

16. “ECI Lightsoft Network Management Solutions General Description Handbook,” 2nd Edition, ECI, June 2006.

17. “Marconi OMS 3200 Optical Multiservice Core Switch,” Marconi, http://archive.ericsson.net/service/internet/picov/get?DocNo=3/28701-FGC101904&Lang=EN#search=%22marconi%207712%22, last accessed 23 September 2006.

18. Walter Goralski, SONET/SDH, 3rd Edition, McGraw Hill/Osborne, Berkeley CA, 2002

19. OPNET Technologies Inc., *http://www.opnet.com*, last accessed 23 September 2006.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Chairman, Code EC
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

4. Ms. Rosemary Wenchel
   Chief Scientist, Naval Security Group Command
   Fort Meade, Maryland

5. Lieutenant Michael Herlands
   Naval Security Group Command
   Fort Meade, Maryland

6. Mr. Bryan Haas
   Laboratory for Telecommunication Science
   Fort Meade, Maryland

7. Professor John C. McEachen
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California

8. Professor Randy L. Borchardt
   Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, California